SOPHOS

simple + secure

Sophos Mobile Control
Administratorhandbuch

Produktversion: 3
Stand: Januar 2013

Inhalt

1 Über Sophos Mobile Control....4
2 Über die Sophos Mobile Control Web-Konsole....7
3 Wichtige Schritte für das Management von Geräten mit der Web-Konsole....9
4 Anmelden an der Sophos Mobile Control Web-Konsole....10
5 Die Benutzeroberfläche der Web-Konsole....12
6 Benutzen der Startseite....15
7 Erstellen neuer Web-Konsolen-Benutzer....19
8 Konfigurieren eines technischen Kontakts....20
9 Konfigurieren von persönlichen Einstellungen....21
10 Konfigurieren von Kennwortrichtlinien....22
11 Konfigurieren von plattformspezifischen Einstellungen....24
12 Konfigurieren von Compliance-Einstellungen....27
13 Konfigurieren der Provisionierung per E-Mail....34
14 Hinzufügen von Geräten zu in Sophos Mobile Control....36
15 Provisionieren von Geräten über die Sophos Mobile Control Web-Konsole....40
16 Mit Softwarepaketen und Applikationen arbeiten....43
17 Mit Konfigurationen (Profilen) arbeiten....51
18 Mit Auftragspaketen arbeiten....78
19 Mit Kommandopaketen arbeiten....81
20 Konfigurieren der Benutzung des Self Service Portal für Endbenutzer....84
21 Verwalten von Geräten im Inventar....91
22 Einsehen von Aufträgen in der Web-Konsole....104
23 Berichte....109
24 Geräte-Backups....111
25 Senden von Nachrichten an Geräte....113
26 Verwaltung von Sophos Mobile Security über Sophos Mobile Control....114

27 Anhang: Allgemeine Schaltflächen in der Web-Konsole.....119
28 Technischer Support.....121
29 Rechtliche Hinweise.....122

1 Über Sophos Mobile Control

Sophos Mobile Control ist eine Device Management Lösung für Mobilgeräte wie Smartphones und Tablets. Sophos Mobile Control hilft Ihnen, Ihre Unternehmensdaten durch die Verwaltung und Steuerung von Apps und Sicherheitseinstellungen zu schützen. Sophos Mobile Control ermöglicht Konfiguration, Software-Verteilung, Definition von Sicherheitseinstellungen und viele andere Mobile Device Management Funktionen bei Mobilgeräten.

Das Sophos Mobile Control System besteht aus einer Server- und einer Client-Komponente, die über Datenverbindungen und Textnachrichten kommunizieren.

Der Sophos Mobile Control Client lässt sich schnell und einfach installieren und verwalten. Dies wird durch Over-the-air-Setup und Konfiguration über die Sophos Mobile Control Web-Konsole erreicht.

Mit dem Sophos Mobile Control Self Service Portal für Ihre Benutzer können Sie IT-Aufwände reduzieren, indem Sie die Benutzer dazu berechtigen, Ihre eigenen Geräte zu registrieren und andere Aufgaben auszuführen. Hierzu ist keine Unterstützung durch den Helpdesk erforderlich.

Sophos Mobile Control unterstützt derzeit folgende Plattformen für Mobilgeräte:

- Android
- Apple iOS
- Windows Mobile
- BlackBerry (über BlackBerry Enterprise Server)

Hinweis: Für BlackBerry-Geräte werden nur bestimmte Funktionen unterstützt. Das Self Service Portal unterstützt BlackBerry-Geräte nicht.

Die unterstützten Funktionen können je nach Plattform variieren. Im *Sophos Mobile Control Technical Guide* (Englisch) finden Sie eine Matrix der für die verschiedenen Plattformen unterstützten Features.

1.1 Sophos Mobile Control als lokale Installation und as a Service

Sophos Mobile Control wird in zwei Liefermodellen angeboten:

- **Sophos Mobile Control für die lokale Installation**

  Mit einer lokalen Installation behalten Sie alle Ihre Daten im Haus und auf Ihrem Server. Diese Variante ist für eine große Anzahl an Benutzern gedacht und bietet erweiterte Managementfunktionen, zum Beispiel:

  - Steuerung des Zugriffs auf Unternehmens-E-Mails
  - Automatische Zuweisung von Geräten zu vorhandenen Gruppen über Ihr Directory
  - Kundenverwaltung mit dem Superadministrator-Kunden, siehe *Sophos Mobile Control Super Administrator Guide* (Englisch).
  - BlackBerry-Unterstützung (über BlackBerry Enterprise Server) zusätzlich zum Device Management für iOS, Android und Windows Mobile

- Konfiguration von Backups für Android-Geräte und Windows Mobile Geräte

- **Sophos Mobile Control as a Service**

  Für unsere Software as a Service Version ist auf Ihrer Seite keine Hardware erforderlich. Sophos Mobile Control wird nicht am Unternehmensstandort installiert. Sophos Mobile Control as a Service ist ideal bei eingeschränkten Ressourcen im IT-Bereich. Für die Installation und den Betrieb von Sophos Mobile Control sind keine Ressourcen erforderlich. Wie bei einer lokalen Installation verwaltet ein Administrator die Geräte über die Web-Konsole. Mit Sophos Mobile Control as a Service können Sie bei kleineren Benutzergruppen schnell und einfach mit Sophos Mobile Control starten.

Die Unterschiede zwischen lokalen Installationen und Sophos Mobile Control as a Service sind in diesem Handbuch gekennzeichnet.

1.2 Einleitung

Dieses Handbuch beschreibt die Benutzung der Sophos Mobile Control Administrations-Web-Konsole.

Eine Beschreibung der Sophos Mobile Control Installation finden Sie im *Sophos Mobile Control Installation Guide* (Englisch).

Hinweis: Der in diesem Handbuch beschriebene Installationsvorgang ist für Sophos Mobile Control as a Service nicht relevant.

Informationen zur Benutzung der Sophos Mobile Control Web-Konsole als Superadministrator für das Kundenmanagement finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

Hinweis: Dieses Handbuch ist für Sophos Mobile Control as a Service nicht relevant. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

Eine Beschreibung der wichtigsten Schritte für die Erstkonfiguration finden Sie in den *Sophos Mobile Control und Sophos Mobile Control as a Service Startup-Anleitungen*.

Informationen zur Benutzung des Sophos Mobile Control Self Service Portal finden Sie in den *Sophos Mobile Control Benutzerhandbüchern für Android, Apple iOS und Windows Mobile*.

1.2.1 Terminologie

In diesem Handbuch werden folgende Begriffe verwendet:

Begriff	Erklärung
Gerät	Das Mobilgerät, dass verwaltet werden soll (zum Beispiel Smartphone oder Tablet).
Sophos Mobile Control client	Die Sophos Mobile Control Client Komponente, die auf dem Gerät installiert ist.
Endbenutzer	Der Endbenutzer des Geräts.

Begriff	Erklärung
Server	Die zentrale Komponente in der Sophos Mobile Control Architektur.
Web-Konsole	Die Web-Oberfläche des Servers, die zur Verwaltung der Geräte benutzt wird.
Kunde	Der Mandant, der Geräte verwaltet.
Provisionierung (Ersteinrichtung)	Der Vorgang der Ausstattung von Geräten mit Sophos Mobile Control.
Self Service Portal (SSP)	Die Sophos Mobile Control Web-Schnittstelle, mit dem Endbenutzer ihre eigenen Geräte registrieren und andere Aufgaben ausführen können. Hierzu ist keine Unterstützung durch den Helpdesk erforderlich.
Sophos Mobile Security	Eine Security App für Android-Mobiltelefone und Tablets, die von Sophos Mobile Control aus verwaltet werden kann. Sophos Mobile Security Management ist ein optionales Modul von Sophos Mobile Control. Zum Verwalten der Sophos Mobile Security App von Sophos Mobile Control aus muss eine Lizenz verfügbar sein. Diese Lizenz muss in der Sophos Mobile Control Web-Konsole aktiviert werden.
SMSec	Abkürzung für Sophos Mobile Security, die in der Benutzeroberfläche von Sophos Mobile Control verwendet wird.

2 Über die Sophos Mobile Control Web-Konsole

Die Sophos Mobile Control Web-Konsole ist das zentrale Instrument für das Management von Geräten mit Sophos Mobile Control. Sie ist die Web-Schnittstelle für den für das Device Management benutzten Server. Mit der Web-Konsole können Sie eine unternehmensweite Richtlinie für die Benutzung von Mobilgeräten implementieren und sie auf die in Sophos Mobile Control registrierten Geräte anwenden.

Hinweis: Aufgrund der unterschiedlichen Betriebssysteme für Mobilgeräte variieren die jeweils unterstützten Features. Im *Sophos Mobile Control Technical Guide* (Englisch) finden Sie eine Matrix der für die verschiedenen Gerätetypen unterstützten Features.

In der Sophos Mobile Control Web-Konsole können Sie

- das System konfigurieren,
- Geräte in Sophos Mobile Control registrieren,
- neue Geräte provisionieren,
- Software-Pakete auf registrierten Geräten installieren,
- Konfigurationen (Profile) und Sicherheitsrichtlinien für Geräte definieren,
- Auftragspakete zum Bündeln mehrerer Aufgaben für Mobilgeräte erstellen und sie in einer Transaktion übertragen,
- spezifische Sophos Mobile Control Client-Kommandopakete definieren, die in einem Vorgang an Geräte übertragen werden,
- administrative Aufgaben bei Geräten durchführen, zum Beispiel den Passcode für Geräte zurücksetzen, Geräte bei Verlust oder Diebstahl sperren oder zurücksetzen, Geräte deregistrieren,
- Daten-Backups für Android-Geräte und Windows Mobile Geräte konfigurieren,

  Hinweis: Backups werden für Sophos Mobile Control as a Service nicht unterstützt.

- Berichte erstellen und einsehen und den Datenverkehr von Geräten überwachen,
- Nachrichten an Geräte senden

2.1 Voraussetzungen

Damit Sie die Sophos Mobile Control Web-Konsole benutzen können, müssen folgende Voraussetzungen erfüllt sein:

- Sie benötigen einen mit dem Internet verbundenen Computer mit einem Internet-Browser. Informationen zu den unterstützten Browsern und den relevanten Versionen finden Sie in den *Sophos Mobile Control Release Notes*.
- In der Web-Konsole muss ein Kunde (ein Mandant, dessen Geräte in Sophos Mobile Control verwaltet werden) vorhanden sein. Kunden werden von Superadministratoren erstellt. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

Hinweis: Für Sophos Mobile Control as a Service wird ein Kunde vordefiniert. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

- Sie benötigen ein Sophos Mobile Control Benutzerkonto und die relevanten Anmeldedaten für die Anmeldung an der Web-Konsole. Die Anmeldedaten bestehen aus Kunde, Benutzer und Kennwort. Für weitere Informationen siehe *Erste Anmeldung* (Seite 10).

2.2 Benutzerrollen

Die Benutzer der Web-Konsole können unterschiedliche Rollen haben. Sie können diese Rollen zuweisen, wenn Sie neue Benutzer in der Web-Konsole anlegen, siehe *Erstellen neuer Web-Konsolen-Benutzer* (Seite 19).

Die in der Web-Konsole verfügbaren Module/Funktionen richten sich nach der Benutzerrolle.

Sie können folgende Benutzerrollen zuweisen:

Benutzerrolle	Beschreibung
Administrator	Hat die Berechtigung, alle verfügbaren Aktionen auszuführen.
Benutzer	Ist zur Durchführung von Aktionen berechtigt, die für die Installation und Verwaltung eines Mobilgeräts erforderlich sind. Die Berechtigungen umfassen jedoch nicht grundlegende Einstellungen (z. B. Ändern eines Client-Pakets oder einer Vorlage).
Helpdesk	Diese Rolle ist nur für Support-Zwecke gedacht. Sie hat nur eingeschränkte Berechtigungen (z. B. Installation von Softwarepaketen). Diese Rolle hat keinen Zugriff auf kritische Funktionen, zum Beispiel die Definition von Einstellungen und das Erstellen, Löschen oder Bearbeiten von Geräten/Gerätegruppen, Paketen und Profilen.

Wenn Sie weitere Benutzerrollen benötigen, wenden Sie sich bitte an den Sophos Support.

3 Wichtige Schritte für das Management von Geräten mit der Web-Konsole

Sophos Mobile Control bietet eine breite Palette von Mobile Device Management Funktionen je nach Gerätetyp, unternehmensweiten Sicherheitsrichtlinien und spezifischen Anforderungen im Unternehmen.

Die wichtigsten Schritte für das Management von Mobilegeräten mit Sophos Mobile Control sind:

- Konfigurieren von plattformspezifischen Einstellungen
- Konfigurieren von Compliance-Einstellungen für Geräte in der Web-Konsole
- Konfigurieren der Provisionierung über E-Mail für Geräte, die SMS nicht unterstützen, z. B. iPads.
- Erstellen von Gerätegruppen

  Gerätegruppen dienen zur Kategorisierung von Geräten. Sie vereinfachen die Verwaltung von Geräten, da in den meisten Device Management Funktionen entweder eine komplette Gruppe oder Einzelgeräte ausgewählt werden können.

- Registrierung und Provisionierung von Geräten

  Geräte können entweder von Administratoren über die Web-Konsole, oder von Geräteendbenutzern über das Self Service Portal registriert und provisioniert werden. In der Web-Konsole können Sie Einstellungen für das Self Service Portal konfigurieren und Self Service Portal Benutzer verwalten.

- Einrichten von Konfigurationen und Sicherheitseinstellungen für Geräte in der Web-Konsole
- Erstellen von Auftragspaketen für die Self Service Portal Konfiguration
- Konfigurieren der Benutzung des Self Service Portal für Endbenutzer
- Anwenden von neuen oder aktualisierten Konfigurationen und Sicherheitseinstellungen auf registrierte Geräte

4 Anmelden an der Sophos Mobile Control Web-Konsole

4.1 Erste Anmeldung

Voraussetzung: In der Sophos Mobile Control Web-Konsole wurde in Benutzerkonto für Sie erstellt und Sie haben die Benutzeranmeldedaten (Kunde, Benutzer und einmal zu verwendendes Kennwort) für dieses Konto. Das Benutzerkonto kann vom Superadministrator während der Sophos Mobile Control Installation, oder von einem anderen Administrator-Benutzer der Web-Konsole angelegt worden sein. Weitere Informationen zum Superadministrator finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Für weitere Informationen zum Erstellen neuer Web-Konsolen-Benutzer siehe *Erstellen neuer Web-Konsolen-Benutzer* (Seite 19).

Hinweis: Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt. Informationen zur ersten Anmeldung an Sophos Mobile Control as a Service finden Sie in der *Sophos Mobile Control as a Service Startup-Anleitung*.

1. Öffnen Sie die Web-Konsole.

   Der Web-Konsole-Anmeldedialog wird angezeigt.

2. Geben Sie **Kunden**, **Benutzer** Namen und das einmal zu verwendende **Kennwort** ein und klicken Sie auf **Einloggen**.

   Sie werden an der Sophos Mobile Control Web-Konsole angemeldet und dazu aufgefordert, Ihr Kennwort zu ändern.

3. Geben Sie ein neues Kennwort ein, bestätigen Sie es und klicken Sie auf die **Speichern** Schaltfläche.

Eine Meldung bestätigt, dass die Änderungen gespeichert wurden. Sie können nun das neue Kennwort zum Anmelden verwenden.

4.2 Anmeldung

1. Öffnen Sie die Web-Konsole.

   Der Web-Konsole-Anmeldedialog wird angezeigt.

2. Geben Sie **Kunden**, **Benutzer** Namen und **Kennwort** ein und klicken Sie auf **Einloggen**.

Sie werden an der Web-Konsole angemeldet. Die **Startseite** Ansicht des Kunden, an dem Sie sich angemeldet haben, wird angezeigt.

4.3 Kennwort-Recovery

Wenn Sie Ihr Kennwort für die Anmeldung an der Web-Konsole vergessen haben, können Sie es zurücksetzen, um ein neues Kennwort zu erhalten.

1. Klicken Sie im **Anmeldedialog** der Web-Konsole auf **Kennwort vergessen?**.

   Der **Kennwort zurücksetzen** Dialog wird angezeigt.

2. Geben Sie Ihre Informationen in den Feldern **Kunde** und **Benutzer** ein und klicken Sie auf **Zurücksetzen**.

   Sie erhalten eine E-Mail mit einem Link zum Zurücksetzen Ihres Kennworts.

3. Klicken Sie auf den Link.

   Der Anmeldedialog mit einer Meldung, dass Ihnen eine E-Mail mit einem neuen Kennwort zugesendet wurde, wird angezeigt. Die zweite E-Mail enthält ein per Zufall generiertes Kennwort.

4. Geben Sie das Kennwort ein, um sich anzumelden.

Sie werden an der Web-Konsole angemeldet und dazu aufgefordert, Ihr Kennwort zu ändern.

4.4 Abmelden

Um sich von der Web-Konsole abzumelden, klicken Sie auf die blaue **Abmelden** Schaltfläche im Header.

5 Die Benutzeroberfläche der Web-Konsole

Die Benutzeroberfläche der Web-Konsole besteht aus dem Header oben, der Menüleiste auf der linken Seite und der jeweiligen Ansicht in der Mitte:

- **Header**

  Im Header stehen folgende Schaltflächen zur Verfügung.

  Hinweis: Wenn Sie mit Ihrem Mauszeiger über eine Schaltfläche fahren, wird ein Tooltip mit dem Namen der Schaltfläche oder mit weiteren Informationen angezeigt.

Schaltfläche	Name	Beschreibung
	Filter	Öffnet die Filterfunktion. Mit der Filterfunktion lässt sich die Anzahl an Posten reduzieren, die in einer Liste angezeigt werden. Je nach der Ansicht, von der aus Sie die Filterfunktion öffnen, stehen unterschiedliche Filter zur Verfügung. Folgende Filter sind verfügbar: Gerätefilter, Gerätegruppenfilter, Softwarefilter und Auftragsfilter. Für weitere Informationen siehe *Filter* (Seite 14). **Hinweis:** Diese Schaltfläche wird nur angezeigt, wenn sich eine Ansicht filtern lässt.
	Aufheben	Diese Schaltfläche wird angezeigt, wenn Sie einen Filter gesetzt haben. Sie hebt einen aktiven Filter wieder auf.
	Startseite	Öffnet die Homepage mit der **Startseite** Ansicht.
	Hilfe	Öffnet einen Link zur Sophos Mobile Control Dokumentation-Website. Auf dieser Website stehen alle Handbücher für Sophos Mobile Control zur Verfügung.
	Abmelden	Meldet den aktuell angemeldeten Benutzer ab.

- **Menüleiste**

  Die Menüleiste auf der linken Seite der Benutzeroberfläche zeigt alle verfügbaren Sophos Mobile Control Module (zum Beispiel **Inventar**) und deren Funktionen (zum Beispiel **Geräte** unter **Inventar**). Mit der Menüleiste können Sie zwischen Modulen und Funktionen navigieren. Klicken Sie auf ein Modul, um eine Ansicht zu öffnen, die die Modulfunktionen mit einer kurzen Beschreibung zeigt. Klicken Sie auf eine Funktion, um sie direkt zu öffnen.

- **Ansicht**

Die Ansicht der Web-Konsole ändert sich je nach benutztem Modul oder benutzter Funktion. Wenn Sie sich an der Web-Konsole anmelden, wird die **Startseite** Ansicht für den Kunden angezeigt, an dem Sie sich angemeldet haben. Für weitere Informationen siehe *Benutzen der Startseite* (Seite 15).

Hinweis: Die Funktionen, Module und Schaltflächen, die in der Web-Konsole verfügbar sind, richten sich nach der Rolle des angemeldeten Benutzers, siehe *Benutzerrollen* (Seite 8). Für Superadministratoren zeigt die Web-Konsole eine spezifische Ansicht für den Superadministrator-Kunden. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

5.1 Tabellen

Die Web-Konsole basiert zum größten Teil auf Tabellen mit Einträgen, bei denen Sie administrative Aufgaben durchführen können. Um die Benutzung dieser Tabellen zu vereinfachen, werden alle angezeigten Einträge standardmäßig in 20 Einträge pro Seite gruppiert. Sie können diese Einstellung nach Ihren Anforderungen ändern, siehe *Konfigurieren von persönlichen Einstellungen* (Seite 21).

Mit den Steuerelementen unterhalb einer Tabelle können Sie durch die Tabellenseiten blättern. In vielen Tabellen lassen sich die angezeigten Einträge sortieren. Felder, die für die Sortierung verwendet werden können, zeigen kleine Pfeilsymbole. Klicken Sie auf die Pfeilsymbole, um die Einträge nach dem ausgewählten Feld zu sortieren.

In den meisten Tabellen können Sie Aktionen bei den aufgelisteten Einträgen mit den Aktionssymbolen ausführen, die neben den Einträgen angezeigt werden. Die angezeigten Symbole richten sich nach der ausgewählten Tabelle und in den meisten Fällen auch nach dem Status des jeweiligen Eintrags.

Die Aktionssymbole lösen folgende Aktionen aus:

Symbol	Beschreibung
	Details zu diesem Eintrag anzeigen.
	Eintrag bearbeiten.
	Eintrag löschen.
	Dieses Symbol wird bei Softwarepaketen angezeigt. Klicken Sie auf das Symbol, um das Softwarepaket von der Web-Konsole herunterzuladen, siehe *Herunterladen von Softwarepaketen aus der Web-Konsole* (Seite 44).

5.2 Schaltflächen

In der Web-Konsole wird eine Reihe von Funktionsschaltflächen benutzt. Wenn Sie mit Ihrem Mauszeiger über eine Schaltfläche fahren, wird ein Tooltip mit dem Namen der Schaltfläche

oder mit weiteren Informationen angezeigt. In diesem Administratorhandbuch werden die in den Tooltips angegebenen Schaltflächennamen verwendet. Für eine illustrierte Übersicht zu allen Funktionsschaltflächen mit den jeweiligen Namen siehe *Anhang: Allgemeine Schaltflächen in der Web-Konsole* (Seite 119).

5.3 Filter

Mit Filtern lässt sich die Anzahl an in Listen angezeigten Einträgen nach definierten Kriterien einschränken. Um den Filter zu öffnen, klicken Sie auf die **Filter** Schaltfläche im Header der Web-Konsole. Die Web-Konsole bietet vier verschiedene Filter:

- Gerätefilter, siehe *Anwenden des Gerätefilters* (Seite 93).
- Gerätegruppenfilter, siehe *Anwenden des Gerätegruppenfilters* (Seite 96).
- Softwarefilter, siehe *Anwenden des Softwarefilters* (Seite 47)
- Auftragsfilter, siehe *Anwenden des Auftragsfilters* (Seite 105).

Die Filter gelten nicht nur für die derzeit angezeigte Funktion, sondern für alle Funktionen, bei denen Einträge dieses Typs aufgelistet werden.

Hinweis: Denken Sie daran, Filter manuell wieder aufzuheben, wenn sie nicht mehr benötigt werden. Andernfalls enthalten Listen oder Berichte unter Umständen nicht die erwarteten Ergebnisse.

6 Benutzen der Startseite

Die **Startseite** ist die erste Ansicht, die angezeigt wird, wenn Sie sich an der Web-Konsole anmelden. Die **Startseite** gibt Ihnen einen Überblick zu dem Kunden, an dem Sie sich angemeldet haben, und zu den für diesen Kunden registrierten Geräten. Sie bietet auch direkten Zugriff auf die Geräte. Darüber hinaus steht auf der **Startseite** eine Reihe von Funktionsschaltflächen zur Verfügung.

Um aus anderen Ansichten zur **Startseite** Ansicht zurückzukehren, klicken Sie auf die **Startseite** Schaltfläche im Header der Web-Konsole.

6.1 Benutzen der Schaltflächen auf der Startseite

Die **Startseite** bietet eine Reihe von Funktionsschaltflächen für den Zugriff auf wichtige Management-Funktionen. Wenn Sie mit Ihrem Mauszeiger über eine Schaltfläche fahren, wird ein Tooltip mit dem Namen der Schaltfläche angezeigt.

- **Einstellungen**

  Klicken Sie auf diese Schaltfläche, um eine Reihe von Einstellungen für die Benutzung von Sophos Mobile Control zu definieren, zum Beispiel persönliche Einstellungen, Kennwortrichtlinien oder Einstellungen für das Self Service Portal.

- **Ändern des Kennworts**

  Klicken Sie auf diese Schaltfläche, um Ihr Kennwort für die Anmeldung an die Web-Konsole zu ändern.

- **Benutzerverwaltung**

  Klicken Sie auf diese Schaltfläche, um die Benutzer der Sophos Mobile Control Web-Konsole zu verwalten. Für weitere Informationen siehe *Erstellen neuer Web-Konsolen-Benutzer* (Seite 19).

- **Interne Benutzerverwaltung**

  Hinweis: Diese Schaltlfläche steht nur für Kunden zur Verfügung, für die die interne Verwaltung von Self Service Portal Benutzern konfiguriert wurde. Ob für einen Kunden die interne Benutzerverwaltung oder die LDAP-Benutzerverwaltung für Self Service Portal Benutzer verwendet wird, wird für lokale Installationen beim Erstellen des Kunden festgelegt. Weitere Informationen zum Erstellen von Kunden für lokale Sophos Mobile Control Installationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt. Für Sophos Mobile Control as a Service werden Kunden vordefiniert. Hier wird die interne Benutzerverwaltung angewendet.

  Klicken Sie auf diese Schaltfläche, um die Benutzer des Sophos Mobile Control Self Service Portal zu verwalten. Für weitere Informationen siehe *Verwalten von Self Service Portal Benutzern* (Seite 88).

- **Technischer Kontakt**

Klicken Sie auf diese Schaltfläche, um die Informationen zum technischen Kontakt anzuzeigen. Diese Informationen beziehen sich auf IT-Ansprechpartner, die bei Fragen oder Problemen weiterhelfen. Nur Benutzer mit der Benutzerrolle **Administrator** können die Informationen zum technischen Kontakt bearbeiten. Für weitere Informationen siehe *Konfigurieren eines technischen Kontakts* (Seite 20).

- **Geräterichtlinien**

  Klicken Sie auf diese Schaltfläche, um Compliance-Überprüfungen für Geräte zu konfigurieren. Für weitere Informationen siehe *Konfigurieren von Compliance-Einstellungen* (Seite 27).

- **Berichte**

  Klicken Sie auf diese Schaltfläche, um einen graphischen Bericht zum Inventarstatus zu öffnen. Für weitere Informationen siehe *Erstellen eines graphischen Berichts zu Geräten* (Seite 109).

6.2 Informationen auf der Startseite

Die **Startseite** zeigt folgende Informationen:

- Kunde, an dem sich der Benutzer angemeldet hat.
- Derzeit angemeldeter Benutzer mit Benutzerrolle (zum Beispiel **Administrator**).
- Anzahl an registrierten Geräten
- Anzahl an lizensierten Geräten
- Lizenzablaufdatum
- Wenn für den Kunden eine Sophos Mobile Security Lizenz verfügbar ist, wird eine zweite Zeile mit Lizenzinformationen für Sophos Mobile Security angezeigt. Sophos Mobile Security Management ist ein optionales Modul von Sophos Mobile Control. Für weitere Informationen siehe *Verwaltung von Sophos Mobile Security über Sophos Mobile Control* (Seite 114).

Außerdem werden Informationen zu den registrierten Geräten in drei Bereichen angezeigt:

- **Gerätestatus**

  Zeigt den Status der registrierten Geräte:

Zeile	Beschreibung
Compliant	Zeigt die Anzahl an Geräten, die den aktuellen Compliance-Einstellungen entsprechen.
Nicht Compliant	Zeigt die Anzahl an Geräten, die den aktuellen Compliance-Einstellungen nicht entsprechen.
Managed	Zeigt die Anzahl an derzeit durch Sophos Mobile Control verwalteten Geräte.

Zeile	Beschreibung
Nicht Managed	Zeigt die Anzahl an Geräten, die derzeit zwar bei Sophos Mobile Control registriert sind, jedoch nicht verwaltet werden.
Checked Out (iOS)	Zeigt die Anzahl an iOS-Geräten, bei denen Benutzer das Mobile Device Management Profil manuell entfernt haben. In diesem Fall versucht das iOS-Gerät, den Server zu benachrichtigen. **Hinweis:** Das iOS Feature "Checkout" wird ab iOS 5 unterstützt.
SSP-Konfiguration abgeschlossen	Zeigt die Anzahl an Geräten, bei denen die Konfiguration über das Self Service Portal abgeschlossen wurde. Mit dem Service Portal können Endbenutzer ihre Geräte selbst registrieren. Für weitere Informationen zum Konfigurieren von Einstellungen für die Benutzung des Self Service Portal, siehe *Konfigurieren von Self Service Portal Einstellungen* (Seite 85).
SSP-Konfiguration in Bearbeitung	Zeigt die Anzahl an Geräten, bei denen die Konfiguration über das Self Service Portal in Bearbeitung ist.
SSP-Konfiguration in fehlgeschlagen	Zeigt die Anzahl an Geräten, bei denen die Konfiguration über das Self Service Portal fehlgeschlagen ist.
Firmengeräte	Zeigt die Anzahl an registrierten Firmengeräten
Private Geräte	Zeigt die Anzahl an registrierten Privatgeräten.

- **Plattformen**

  Zeigt die Anzahl an Geräten für die einzelnen Betriebssysteme.

- **Gerätegruppen**

  Zeigt die verfügbaren Gerätegruppen mit der jeweiligen Anzahl an zugehörigen Geräten.

Wenn Sie in den drei Gerätebereichen auf eine Tabellenzeile klicken, wird die Geräteliste gefiltert auf den relevanten Eintrag angezeigt. Sie können so direkt von der **Startseite** aus auf die registrierten Geräte in den verschiedenen Kategorien zugreifen.

Hinweis: Denken Sie daran, den Filter manuell wieder aufzuheben, wenn er nicht mehr benötigt wird. Andernfalls enthalten Listen oder Berichte unter Umständen nicht die erwarteten Ergebnisse.

Sie können auf den Link **Privacy Policy and Terms and Conditions** unter den drei Gerätebereichen klicken, um rechtliche Informationen einzusehen.

7 Erstellen neuer Web-Konsolen-Benutzer

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Benutzerverwaltung**.

   Die **Benutzer anzeigen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neuen Benutzer anlegen**.

   Die **Benutzer bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Loginnamen** für den neuen Benutzer ein.
4. Wählen Sie im Feld **Rolle** die Benutzerrolle:

   - **Administrator**
   - **User**
   - **Helpdesk**

   Für weitere Informationen siehe *Benutzerrollen* (Seite 8).

5. Geben Sie den **Nachnamen** und den **Vornamen** des neuen Benutzers ein.
6. Geben Sie die **E-Mail** Adresse des neuen Benutzers ein.
7. Geben Sie ein einmal zu verwendendes **Kennwort** für die erste Anmeldung an der Web-Konsole ein und bestätigen Sie es.
8. Klicken Sie auf die **Speichern** Schaltfläche.

Der neue Benutzer wird angelegt und in der **Benutzer anzeigen** Ansicht angezeigt. Geben Sie die Benutzeranmeldedaten (Benutzer, Kunde und einmal zu verwendendes Kennwort) an den neuen Benutzer weiter. Der neue Benutzer kann sich an der Web-Konsole anmelden und wird zum Ändern seines Kennworts aufgefordert.

8 Konfigurieren eines technischen Kontakts

In der Web-Konsole können Sie Informationen zu einem technischen Kontakt konfigurieren, um Benutzer bei Fragen oder Problemen zu unterstützen.

Voraussetzung: Zum Bearbeiten der Informationen zum technischen Kontakt benötigen Sie die Benutzerrolle **Administrator**.

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Technischer Kontakt**.

   Die **Technischer Kontakt** Ansicht wird angezeigt.

2. Klicken Sie auf die **Bearbeiten** Schaltfläche.

   Die Felder in der **Technischer Kontakt** Ansicht lassen sich nun bearbeiten.

3. Geben Sie die erforderlichen Informationen für den technischen Kontakt ein. Unter **Zusatzinformation** können Sie zusätzliche Informationen für die Unterstützung von Benutzern bei Fragen oder Problemen eingeben.
4. Klicken Sie auf die **Speichern** Schaltfläche.

Die Informationen zum technischen Kontakt werden angezeigt, wenn Benutzer auf der **Startseite** auf die Schaltfläche **Technischer Kontakt** klicken. Für Endbenutzer werden die Informationen zum technischen Kontakt in der Sophos Mobile Control App auf iOS- und Android-Geräten angezeigt. Sie werden auch dann angezeigt, wenn Endbenutzer im Self Service Portal auf die **Hilfe** Schaltfläche klicken.

9 Konfigurieren von persönlichen Einstellungen

Sie können persönliche Einstellungen für die Benutzung der Sophos Mobile Control Web-Konsole definieren.

Hinweis: Diese Einstellungen sind benutzerspezifisch. Sie müssen für jedes Benutzerkonto separat definiert werden.

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Einstellungen**.

   Die **Einstellungen** Ansicht wird angezeigt.

2. Konfigurieren Sie in der **Persönlich** Registerkarte folgende Einstellungen:

   a) Wählen Sie im **Datensätze pro Tabellenseite** Feld die maximale Anzahl an Datensätzen aus, die in der Web-Konsole pro Seite angezeigt werden sollen. Sie können zwischen **20** und **100** Datensätzen auswählen.

   b) Wählen Sie unter **Aktivierte Plattformen** die Plattformen aus, die Sie in der Web-Konsole benutzen möchten: **Android**, **Blackberry**, **iOS** und/oder **Windows Mobile**. Wenn Sie spezifische Plattformen auswählen, können Sie nur diese Plattformen mit Sophos Mobile Control verwenden. Alle anderen Plattformen werden verborgen. Darüber hinaus werden alle Module und Funktionen verborgen, die für eine spezifische Plattform nicht benötigt werden.

3. Klicken Sie auf die **Speichern** Schaltfläche.
4. Da einige Änderungen in den persönlichen Einstellungen erst nach der nächsten Anmeldung wirksam werden, melden Sie sich von der Web-Konsole ab und melden Sie sich erneut an.

Die neuen persönlichen Einstellungen gelten für Ihr Benutzerkonto.

10 Konfigurieren von Kennwortrichtlinien

Zur Durchsetzung der Sicherheit von Kennwörtern können Sie kundenspezifische Kennwortrichtlinien für Benutzer der Sophos Mobile Control Web-Konsole und des Self Service Portal definieren. Die von Ihnen definierten Kennwortrichtlinien gelten für neue und geänderte Kennwörter.

Hinweis: Die Kennwortrichtlinien gelten nur für Self Service Portal Benutzer, die über die interne Benutzerverwaltung verwaltet werden. Wenn Sie externe Benutzerverwaltung anwenden, gelten die in der externen Benutzerverwaltung definierten Kennwortrichtlinien für die Self Service Portal Benutzer. In diesem Fall gelten die in der Sophos Mobile Control Web-Konsole definierten Kennwortrichtlinien nur für Web-Konsole-Benutzer.

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Einstellungen**.

   Die **Einstellungen** Ansicht wird angezeigt.

2. Wechseln Sie in die Registerkarte **Kennwortrichtlinien**.
3. Definieren Sie unter **Kennwortrichtlinien für Benutzer der SMC Web-Konsole und des SSP** - **Qualität des Kennworts** die folgenden Mindestwerte für das Kennwort:

   - **Minimale Länge des Kennworts** Sie können einen Wert zwischen **4** und **10** auswählen.
   - **Minimale Anzahl von Kleinbuchstaben** Sie können einen Wert zwischen **1** und **10** auswählen.
   - **Minimale Anzahl von Großbuchstaben** Sie können einen Wert zwischen **1** und **10** auswählen.
   - **Minimale Anzahl von Ziffern** Sie können einen Wert zwischen **1** und **10** auswählen.
   - **Minimale Anzahl von Sonderzeichen** Sie können einen Wert zwischen **1** und **10** auswählen.

4. Definieren Sie unter **Kennwortrichtlinien für Benutzer der SMC Web-Konsole und des SSP** - **Einstellungen des Kennworts** die folgenden Einstellungen:

   - **Änderungsintervall** (**Tage**): Sie können einen Wert zwischen **0** (keine Kennwortänderung erforderlich) und **730** Tagen eingeben.
   - **Anzahl der letzten Kennwörter, die nicht benutzt werden dürfen**: Sie können einen Wert zwischen **1** und **10** auswählen.
   - **Maximale Anzahl fehlerhafter Loginversuche**: Sie können einen Wert zwischen **2** und **10** auswählen.

5. Unter **Einstellungen "Kennwort vergessen"-E-Mail** konfigurieren Sie die E-Mails, die an Benutzer gesendet werden sollen, wenn diese das Zurücksetzen ihres Kennworts angefordert haben. Wenn Benutzer das Zurücksetzen ihres Kennworts angefordert haben, erhalten sie eine E-Mail mit einem Link zum Erzeugen eines neuen Kennworts. Wenn sie auf den Link geklickt haben, wird eine zweite E-Mail mit einem einmal zu verwendenden Kennwort an die Benutzer geschickt. Für weitere Informationen siehe *Kennwort-Recovery* (Seite 11).

   a) Geben Sie im **Absender** Feld die E-Mail-Absenderadresse ein.

   b) Geben Sie unter **Einstellungen "Kennwort vergessen"-E-Mail** - **E-Mail mit dem Reset-Link** einen **Betreff** für die erste E-Mail, die an die Benutzer geschickt werden soll,

ein, zum Beispiel "Neues Kennwort für Sophos Mobile Control erzeugen". Definieren Sie im Textfeld den Inhalt der E-Mail. Benutzen Sie den Platzhalter _RESET_TOKEN_LINK_, um einen Link für das Erzeugen eines Kennworts für den Benutzer hinzuzufügen. Dieser Link ist für die Bereitstellung eines neuen Kennworts für den Benutzer erforderlich. Die Platzhalter _RESET_TOKEN_LINK, _LOGINNAME_, _FIRSTNAME_ und _LASTNAME_ werden in der E-Mail durch die entsprechenden Werte ersetzt.

c) Geben Sie unter **Einstellungen "Kennwort vergessen"-E-Mail** - **E-Mail mit dem neuen Kennwort** einen **Betreff** für die zweite E-Mail, die an die Benutzer geschickt werden soll, ein, zum Beispiel "Neues Kennwort für Sophos Mobile Control". Definieren Sie im Textfeld den Inhalt der E-Mail. Benutzen Sie den Platzhalter _NEW_PASSWORD_, um das neue Kennwort für den Benutzer in die E-Mail einzufügen. Dieser Link ist für die Bereitstellung eines neuen Kennworts für den Benutzer erforderlich. Die Platzhalter _NEW_PASSWORD_, _LOGINNAME_, _FIRSTNAME_ und _LASTNAME_ werden in der E-Mail durch die entsprechenden Werte ersetzt.

6. Klicken Sie auf die **Speichern** Schaltfläche.

Die definierten Kennwortrichtlinien gelten für Benutzer der Web-Konsole und des Self Service Portal für diesen Kunden.

11 Konfigurieren von plattformspezifischen Einstellungen

Für bestimmte Plattformen müssen spezifische Einstellungen konfiguriert werden, damit das Management dieser Gerätetypen in Sophos Mobile Control unterstützt wird.

- **Apple iOS**

  Für iOS-Geräte müssen Sie die Benutzung des Apple Push Notification Service durch Hochladen des APNs Keystore in die Web-Konsole aktivieren. Weitere Informationen dazu, wie Sie Ihr APNs Zertifikat für Sophos Mobile Control erhalten, finden Sie in der *Sophos Mobile Control Startup-Anleitung* bzw. in der *Sophos Mobile Control as a Service Startup-Anleitung*.

  Außerdem können Sie die Lokalisieren-Funktion für iOS-Geräte konfigurieren, wenn dies für den Kunden zulässig ist, an dem Sie angemeldet sind. Der Superadministrator kann die iOS-Lokalisieren-Funktion in der Kundenverwaltung aktivieren oder deaktivieren. Weitere Informationen zur Kundenverwaltung finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

  Hinweis: Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt. Für Sophos Mobile Control as a Service werden Kunden vordefiniert.

- **BlackBerry**

  Für die Unterstützung von BlackBerry-Geräten müssen Sie den BlackBerry Enterprise Server in der Web-Konsole angeben.

11.1 Hochladen des Apple Push Notification Keystore

Um das integrierte Mobile Device Management (MDM) Protocol von Geräten mit Apple iOS 4 (oder höher) verwenden zu können, muss Sophos Mobile Control den Apple Push Notification Service (APNs) zum Triggern von iOS-Geräten benutzen. Um den Apple Push Notification Service zu aktivieren, müssen Sie den Apple Push Notification Keystore in die Web-Konsole hochladen. Informationen dazu, wie Sie Ihr APNs Zertifikat für Sophos Mobile Control erhalten, finden Sie in der *Sophos Mobile Control Startup-Anleitung* bzw. in der *Sophos Mobile Control as a Service Startup-Anleitung*.

Voraussetzung: Sie haben Ihr APNs Zertifikat für Sophos Mobile Control erhalten.

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Einstellungen**.

   Die **Einstellungen** Ansicht wird angezeigt.

2. Wechseln Sie in die Registerkarte **iOS APNS**.
3. Suchen Sie nach der APNs-Zertifikatsdatei. Wenn Sie während der Erstellung den vorgeschlagenen Namen nicht geändert haben, sollte diese Datei die Bezeichnung mdm_apns_certificate.pkcs12 haben. Geben Sie das erforderliche Kennwort ein und klicken Sie auf **Übertragen**.

   Wenn die Datei erfolgreich hoch geladen wurde, wird eine Bestätigungsmeldung angezeigt.

4. Klicken Sie auf **Speichern**.

11.2 Konfigurieren der Positionsüberwachung für iOS-Geräte

Wenn die **Position anzeigen** Funktion aktiviert ist, bestimmt die auf iOS-Geräten installierte Sophos Mobile Control App die Position des Geräts und sendet diese an den Sophos Mobile Control Server. Sie können eine Compliance-Einstellung konfigurieren, die sich auf die **Position anzeigen** Funktion bezieht. Somit können Sie sicherstellen, dass der Benutzer der Sophos Mobile Control App gestattet, Positionsdaten abzurufen, siehe *Verfügbare Compliance-Einstellungen* (Seite 28). Die **Position anzeigen** Funktion steht Administratoren in den **Gerät anzeigen** und **Gerät bearbeiten** Ansichten (siehe *Ausführen von administrativen Aufgaben* (Seite 98)) und Endbenutzern im Sophos Mobile Control Self Service Portal (siehe *Sophos Mobile Control Benutzerhandbuch für Apple iOS*) zur Verfügung.

Hinweis: Sie können diese Funktion nur dann für iOS-Geräte konfigurieren, wenn dies für den Kunden zulässig ist, an dem Sie angemeldet sind. Der Superadministrator kann die Funktion in der Kundenverwaltung aktivieren oder deaktivieren. Weitere Informationen zur Kundenverwaltung finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt. In diesem Fall sind die Kunden vordefiniert.

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Einstellungen**.

   Die **Einstellungen** Ansicht wird angezeigt.

2. Wechseln Sie in die Registerkarte **iOS-Client**.
3. Stellen Sie sicher, dass das Feld **Positionsüberwachung aktivieren** ausgewählt ist.
4. Wählen Sie im Feld **Gewünschte Genauigkeit (in Metern)** den Radius für durch die **Position anzeigen** Funktion erfasste Positionsänderungen aus.

   - **100**
   - **1000**
   - **3000**

   Hinweis: Wenn Sie in diesem Feld einen kleinen Radius auswählen, kann sich dies aufgrund einer hohen Anzahl an Positionsabfragen auf die Akku-Laufzeit des Endbenutzergeräts auswirken. Wenn Sie einen großen Radius wählen, kann dies aufgrund der gesendeten Positionsbenachrichtigungen Auswirkungen auf die Server-Auslastung haben.

5. Klicken Sie auf die **Speichern** Schaltfläche.

11.3 Konfigurieren des BlackBerry Enterprise Server

BlackBerry-Geräte werden in Sophos Mobile Control durch den BlackBerry Enterprise Server unterstützt. In der Web-Konsole müssen Sie die URL des BlackBerry Enterprise Server und das Benutzerkonto, das für Sophos Mobile Control benutzt werden soll, angeben.

Hinweis: BlackBerry-Geräte werden für Sophos Mobile Control as a Service nicht unterstützt.

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Einstellungen**.

   Die **Einstellungen** Ansicht wird angezeigt.

2. Wechseln Sie in die Registerkarte **RIM BES**.

3. Geben Sie im **BlackBerry BES URL** Feld die URL des BlackBerry Enterprise Server ein.
4. Geben Sie **Benutzername** und **Kennwort** des Benutzerkontos, das für Sophos Mobile Control verwendet werden soll, ein.
5. Klicken Sie auf die **Speichern** Schaltfläche.

12 Konfigurieren von Compliance-Einstellungen

In der Sophos Mobile Control Web-Konsole können Sie:

- Compliance-Einstellungen und Regeln für alle verfügbaren Gerätetypen (Plattformen) definieren.
- Aktionen festlegen, die ausgeführt werden, wenn Geräte nicht mehr den festgelegten Regeln entsprechen.
- Mehrere Sets mit Compliance-Einstellungen und Regeln definieren und diese Gerätegruppen zuweisen. In Gerätegruppen können Sie unterschiedliche Compliance Sets für Firmengeräte und private Geräte auswählen. Somit können Sie auf verschiedene Gerätegruppen unterschiedliche Sicherheitsstufen anwenden.

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Geräterichtlinien**.

   Die **Compliance-Einstellungen** Listenansicht wird angezeigt.

2. Klicken Sie auf die **Hinzufügen** Schaltfläche.
3. Die **Compliance-Einstellungen** Ansicht mit Registerkarten für alle verfügbaren Gerätetypen wird angezeigt.
4. Geben Sie einen **Namen** und eine **Beschreibung** für das neue Compliance Set ein.
5. Wechseln Sie in die erforderliche Registerkarte.
6. Stellen Sie sicher, dass das Feld **Plattform aktivieren** ausgewählt ist.

   Hinweis: Wenn dieses Feld nicht ausgewählt ist, können die Geräte der Plattform nicht auf Compliance überprüft werden.

7. Konfigurieren Sie unter **Regel** die Compliance-Anforderungen für den ausgewählten Gerätetyp. Für eine Auflistung der pro Gerätetyp verfügbaren Einstellungen, siehe *Verfügbare Compliance-Einstellungen* (Seite 28).
8. Unter **Active Sync sperren** können Sie festlegen, dass der E-Mail-Zugriff automatisch verweigert wird, wenn Geräte nicht den Compliance-Richtlinien entsprechen. Wählen Sie die erforderlichen Kontrolllkästchen neben den entsprechenden Regeln aus.

   Hinweis: Die Steuerung des Zugriffs auf Unternehmens-E-Mails wird in Sophos Mobile Control as a Service nicht unterstützt. Wenn Sie Sophos Mobile Control as a Service benutzen, wird die Spalte **Active Sync sperren** nicht angezeigt.

9. Unter **Admin benachrichtigen** können Sie festlegen, dass Administratoren per E-Mail benachrichtigt werden, wenn Geräte nicht den Compliance-Richtlinien entsprechen. Wählen Sie die erforderlichen Kontrollkästchen neben den entsprechenden Regeln aus.
10. Unter **Auftragspaket übertragen** können Sie Auftragspakete auswählen, die für die entsprechenden **Regel** Einstellungen übertragen werden. Wenn Geräte nicht mit den Regeln übereinstimmen, werden die ausgewählten Auftragspakete automatisch übertragen.

    Hinweis: Sie müssen die Auftragspakete zuerst in der Web-Konsole anlegen. Wenn Sie noch kein Auftragspaket erstellt haben, aktualisieren Sie die Compliance-Einstellungen danach. Für Informationen zur Erstellung eines Auftragspakets siehe *Mit Auftragspaketen arbeiten* (Seite 78).

11. Wenn Sie alle Einstellungen in allen erforderlichen Gerätetyp-Registerkarten konfiguriert haben, klicken Sie auf die **Speichern** Schaltfläche.

    Das neue Compliance Set wird in der **Compliance-Einstellungen** Listenansicht angezeigt.

12. Wenn Sie festgelegt haben, dass Administratoren per E-Mail benachrichtigt werden sollen, wenn Geräte nicht mehr die Compliance-Regeln erfüllen, geben Sie die gewünschten Empfänger unter **Admin E-Mail Empfänger** an. Verwenden Sie im Feld **Admin E-Mail Empfänger** das Zeichen **;** zum Trennen mehrerer Administratoren. Legen Sie unter **Admin E-Mail Zeitplan** einen Zeitplan für die Benachrichtigung fest.
13. Klicken Sie auf die **Speichern** Schaltfläche.

Das neue Compliance Set kann Gerätegruppen zugewiesen werden. Unterschiedliche Compliance Sets für Firmengeräte und private Geräte in Gerätegruppen auswählen.

12.1 Verfügbare Compliance-Einstellungen

Die folgende Tabelle zeigt die Compliance-Einstellungen die Sie für die einzelnen Plattformen unter **Regel** in der jeweiligen **Compliance-Einstellungen** Registerkarte auswählen können.

Einstellung	Beschreibung	Android	iOS	Windows Mobile	BlackBerry
Min. Client-Version	Geben Sie die Sophos Mobile Control Client Mindestversion ein, die auf dem Gerät installiert sein muss.	✓	✓	✓	✗
Root-Rechte erlauben	Wählen Sie aus, ob Geräte mit Root-Rechten zulässig sind.	✓	✗	✗	✗
Jailbreak erlauben	Wählen Sie aus, ob Jailbroken-Geräte zulässig sind.	✗	✓	✗	✗
Passcode erforderlich	Wählen Sie aus, ob für Geräte ein Passcode erforderlich ist:	✗	✓	✗	✗
Non-Market Apps erlauben	Wählen Sie aus, ob Non-Market Apps auf Geräten zulässig sind.	✓	✗	✗	✗

Einstellung	Beschreibung	Android	iOS	Windows Mobile	BlackBerry
Debug Bridge (ADB) erlauben	Wählen Sie aus, ob ADB (Android Debug Bridge) auf Geräten zulässig ist.	✓	✗	✗	✗
Min. OS Version:	Wählen Sie die Mindestversion für das Betriebssystem auf Geräten aus.	✓	✓	✓	✓
Max. Synchronisations-abstand	Geben Sie das maximale Intervall zwischen Synchronisierungs-vorgängen für Geräte an.	✓	✓	✓	✗
Max. Synchronisations-abstand der iOS App	Geben Sie das maximale Intervall zwischen iOS App Synchronisierungs-vorgängen für Geräte an. Weitere Informationen finden Sie im *Sophos Mobile Control Benutzerhandbuch für Apple iOS*.	✗	✓	✗	✗
Max. SMSec-Scanintervall	Dieses Feld wird nur dann angezeigt, wenn für den Kunden Sophos Mobile Security verfügbar ist. Für weitere Informationen siehe *Verwaltung von Sophos Mobile Security über Sophos Mobile Control* (Seite 114). In diesem Feld können Sie den Höchstabstand zwischen Malware	✓	✗	✗	✗

Einstellung	Beschreibung	Android	iOS	Windows Mobile	BlackBerry
	Scans angeben, die von der Sophos Mobile Security App auf dem Gerät durchgeführt werden.				
Malware Apps zugelassen	Dieses Feld wird nur dann angezeigt, wenn für den Kunden Sophos Mobile Security verfügbar ist. Wählen Sie aus, ob Malware Apps auf Geräten zulässig sind.	✗	✗	✗	
Verdächtige Apps zugelassen	Dieses Feld wird nur dann angezeigt, wenn für den Kunden Sophos Mobile Security verfügbar ist. Wählen Sie aus, ob verdächtige Apps auf Geräten zulässig sind.	✓	✗	✗	✗
PUA zugelassen	Dieses Feld wird nur dann angezeigt, wenn für den Kunden Sophos Mobile Security verfügbar ist. Wählen Sie aus, ob PUAs (Potentially Unwanted Apps) auf Geräten zulässig sind.	✓	✗	✗	✗
Hardwareverschlüsselung erforderlich	Wählen Sie aus, ob für Geräte Verschlüsselung erforderlich ist.	✓	✓	✗	✗

Einstellung	Beschreibung	Android	iOS	Windows Mobile	BlackBerry
Data-Roaming erlaubt	Wählen Sie aus, ob für Geräte Daten-Roaming zulässig ist.	✓	✓	✗	✗
App-Lokalisierung erforderlich	Diese Einstellung bezieht sich auf die **Lokalisieren** Funktion für iOS-Geräte. Legen Sie fest, ob der Benutzer der Sophos Mobile Control App gestatten muss, Ortsdaten abzurufen, damit das Gerät compliant ist. Für weitere Informationen, siehe *Konfigurieren der Positionsüberwachung für iOS-Geräte* (Seite 25).	✗	✓	✗	✗
Blacklisted Apps/Whitelisted Apps	Apps auf Geräten zulassen/verbieten. Wählen Sie **Blacklisted Apps** oder **Whitelisted Apps** aus der Dropdown-Liste und klicken Sie auf **Bearbeiten**. Fügen Sie in der **Whitelist/Blacklist bearbeiten** Ansicht die App(s) hinzu, die Sie zulassen/ verbieten möchten, und klicken Sie auf **Übernehmen**. **Hinweis:** Wenn Sie Whitelisted Apps verwenden, können	✓	✓	✓	✓

Einstellung	Beschreibung	Android	iOS	Windows Mobile	BlackBerry
	nur die in der Liste enthaltenen Apps installiert werden.				
Erforderliche Apps	Geben Sie Apps an, die auf den Geräten installiert werden müssen. Klicken Sie auf **Bearbeiten**. Fügen Sie in der **Erforderliche Apps bearbeiten** Ansicht die App(s) hinzu, die Sie als erforderlich definieren möchten, und klicken Sie auf **Übernehmen**.	✓	✓	✓	✓

12.2 Zuweisen von Compliance Sets zu Gerätegruppen

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Gerätegruppen**.

   Die **Gerätegruppen** Ansicht wird angezeigt.

2. Klicken Sie auf das **Bearbeiten** Symbol neben der Gerätegruppe, der Sie Compliance Sets zuweisen möchten.

   In der Web-Konsole steht eine **Default** Gerätegruppe zur Verfügung. Für weitere Informationen zum Erstellen eigener Gerätegruppen siehe *Erstellen von Gerätegruppen* (Seite 36).

3. Wählen Sie unter **Compliance-Einstellungen** in den Feldern **für Firmengeräte** und **für private Geräte** die Compliance Sets, die Sie anwenden möchten.
4. Klicken Sie auf die **Speichern** Schaltfläche.

Die ausgewählten Compliance Sets werden in der **Gerätegruppen** Ansicht für die jeweilige Gerätegruppe unter **Richtlinie für Firmengeräte** und **Richtlinien für private Geräte** angezeigt.

12.3 Compliance-Prüfung bei Geräten

Wenn Sie Compliance-Einstellungen definiert haben, können Sie prüfen, ob registrierte Geräte den definierten Richtlinien entsprechen.

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Geräterichtlinien**.

   Die **Compliance-Einstellungen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Jetzt prüfen**.

Alle registrierten Geräte werden nach den unter **Compliance-Einstellungen** definierten Regeln geprüft. Die festgelegten Aktionen werden ausgeführt. Die **Gerätestatus** Übersicht auf der **Startseite** wird entsprechend aktualisiert.

13 Konfigurieren der Provisionierung per E-Mail

Die Provisionierung von Android-Geräten und Apple iOS Geräten kann über E-Mail anstelle von SMS erfolgen. Dieses Verfahren kann für Geräte benutzt werden, die SMS nicht unterstützen, zum Beispiel iPads.

Voraussetzungen:

- Während der Sophos Mobile Control Installation muss ein Mail-Server konfiguriert werden. Weitere Informationen finden Sie im *Sophos Mobile Control Installation Guide* (Englisch).

  Hinweis: Für Sophos Mobile Control as a Service wird der Mail-Server vordefiniert. Der im Sophos Mobile Control Installation Guide beschriebene Installationsvorgang ist hier nicht relevant.

- Ein E-Mail-Konto (persönliches E-Mail-Konto oder Firmen-E-Mail-Konto) muss auf den Geräten, die provisioniert werden sollen, zur Verfügung stehen.
- Die E-Mail-Adressen müssen beim Hinzufügen zu Sophos Mobile Control (manuell oder über Import) angegeben werden.
- Die Telefonnummer muss beim Hinzufügen der Geräte zu Sophos Mobile Control (manuell oder über Import) mit 0 angegeben werden. Die angegebene E-Mail-Adresse wird nur dann für die Ersteinrichtung benutzt, wenn keine Telefonnummer vorhanden ist.

So konfigurieren Sie die E-Mails, die gesendet werden:

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Einstellungen**.

   Die **Einstellungen** Ansicht wird angezeigt.

2. Wechseln Sie in die **Provisioning per E-Mail** Registerkarte.
3. Geben Sie im **Absender** Feld die E-Mail-Absenderadresse ein.
4. Definieren Sie im **Betreff** Feld einen E-Mail-Betreff. Folgende Platzhalter stehen zur Verfügung:

   - _DEVICENAME_
   - _DEVICEDESCRIPTION_

   Die Platzhalter werden in der an die Geräte gesendeten E-Mail durch die jeweiligen Werte ersetzt.

5. Definieren Sie in den Textfeldern **Inhalt für Android-Geräte** und/oder I**nhalt für iOS-Geräte** den Inhalt der E-Mail. Folgende Platzhalter stehen zur Verfügung:

   - _DOWNLOADLINK_
   - _CONFIG_LINK_
   - _DEVICENAME_
   - _DEVICEDESCRIPTION_

   Die Link-Platzhalter sind Pflicht-Platzhalter. Sie werden in der an die Geräte gesendeten E-Mail durch den jeweiligen Link ersetzt.

6. Klicken Sie auf die **Speichern** Schaltfläche.

Die konfigurierte E-Mail wird an die E-Mail-Konten der Geräte zur Ersteinrichtung gesendet.

14 Hinzufügen von Geräten zu in Sophos Mobile Control

Geräte lassen sich auf folgende Art und Weisen zur Sophos Mobile Control Verwaltung hinzufügen:

- Manuelles Hinzufügen von Geräten in der Web-Konsole
- Importieren von Geräten in einer .csv-Datei in der Web-Konsole
- Ermöglichen der Registrierung von Endgeräten durch Endbenutzer über das Self Service Portal, siehe *Konfigurieren von Self Service Portal Einstellungen* (Seite 85). Mit dem Sophos Mobile Control Self Service Portal für Ihre Benutzer können Sie IT-Aufwände reduzieren, indem Sie die Benutzer dazu berechtigen, Ihre eigenen Geräte zu registrieren und andere Aufgaben auszuführen. Hierzu ist keine Unterstützung durch den Helpdesk erforderlich. Die Geräte werden durch Ausführen von vordefinierten Auftragspaketen provisioniert, siehe *Mit Auftragspaketen arbeiten* (Seite 78).

  Weitere Informationen zur Registrierung von Geräten über das Self Service Portal finden Sie in den *Sophos Mobile Control Benutzerhandbüchern für Android, Apple iOS und Windows Mobile*.

Zur Vereinfachung der Verwaltung lassen sich Geräte gruppieren. Sie können Geräte vorhandenen Gerätegruppen zuordnen, wenn Sie sie zur Sophos Mobile Control Verwaltung hinzufügen. In der Web-Konsole steht eine **Default** Gerätegruppe zur Verfügung. Wenn Sie noch keine eigenen Gerätegruppen definiert haben, können Sie Geräte zu dieser Gruppe hinzufügen.

14.1 Erstellen von Gerätegruppen

Gerätegruppen dienen zur Kategorisierung von Geräten. Sie können Geräte zu Gerätegruppen zuweisen, wenn Sie sie zum Sophos Mobile Control Device Management manuell oder über Import hinzufügen. Für Geräte, die Endbenutzer über das Self Service Portal registrieren, können Sie die Gruppe definieren, zu der diese hinzugefügt werden sollen, siehe *Konfigurieren von Self Service Portal Einstellungen* (Seite 85).

Ein Gerät gehört immer exakt zu einer Gerätegruppe. Gerätegruppen vereinfachen die Verwaltung von Geräten, da in den meisten Device Management Funktionen entweder eine komplette Gruppe oder Einzelgeräte ausgewählt werden können.

Hinweis: Wir empfehlen, nur Geräte mit demselben Betriebssystem zu gruppieren. Gruppen lassen sich dadurch leichter für Installationen und andere betriebssystemspezifische Vorgänge verwenden.

In der Web-Konsole steht eine **Default** Gerätegruppe zur Verfügung. Wenn Sie noch keine eigenen Gerätegruppen definiert haben, können Sie Geräte zu dieser Gruppe hinzufügen.

So erstellen Sie Gerätegruppen:

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Gerätegruppen**.

   Die **Gerätegruppen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neue Gerätegruppe anlegen**.

   Die **Gerätegruppe bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Beschreibung** für die neue Gerätegruppe ein.
4. Unter **Compliance-Einstellungen** können Sie in den Feldern **für Firmengeräte** und **für private Geräte** die Compliance Sets wählen, die Sie anwenden möchten.
5. Klicken Sie auf die **Speichern** Schaltfläche.

Die neue Gerätegruppe wird angelegt und in der **Gerätegruppen** Ansicht angezeigt. Sie können nun Geräte zur neuen Gruppe hinzufügen.

Hinweis: Wenn Sie Geräte zur Gruppe hinzugefügt haben, können Sie die Details zu den Gerätegruppenmitgliedern aufrufen, indem Sie in der **Mitglieder** Tabelle der **Gerätegruppen anzeigen** oder **Gerätegruppen bearbeiten** Ansicht auf das gewünschte Gerät klicken.

Hinweis: Wenn Sie eine Gerätegruppe löschen, werden die Mitglieder der Gruppe in eine andere Gruppe verschoben. Diese muss angegeben werden. Ist keine Gruppe mehr vorhanden, in die die Geräte verschoben werden können, so kann die Gruppe nicht gelöscht werden. Bevor eine Gruppe gelöscht wird, wird eine Warnungsmeldung angezeigt.

14.2 Erstellen eines neuen Geräts

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Geräte**.

   Die **Geräte** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neues Gerät anlegen**

   Die **Gerätevorlage auswählen** Ansicht wird angezeigt.

3. Wählen Sie unter **Vorlage** die Gerätevorlage für den Mobilgerätetyp (zum Beispiel Android) und klicken Sie auf **Weiter**.

   Die **Gerät bearbeiten** Ansicht wird angezeigt.

4. Geben Sie in der **Gerät bearbeiten** Ansicht die folgenden Gerätedetails an:

   a) Geben Sie im Feld **Name** einen eindeutigen Namen für das neue Gerät ein.

   b) Geben Sie im Feld **Beschreibung** eine Beschreibung für das neue Gerät ein.

   c) Wählen Sie unter **Gerätegruppe** die Gerätegruppe, zu der das Gerät hinzugefügt werden soll.

      Hinweis: Hier steht eine **Default** Gerätegruppe zur Verfügung. Wenn Sie noch keine eigenen Gerätegruppen definiert haben, können Sie Geräte zu dieser Gruppe hinzufügen. Für weitere Informationen zum Erstellen eigener Gerätegruppen siehe *Erstellen von Gerätegruppen* (Seite 36).

   d) Geben Sie im **Telefonnummer** Feld die Telefonnummer des neuen Geräts ein. Dieses Feld ist ein Pflichtfeld. Wenn Sie ein Gerät hinzufügen, das keine Telefonnummer hat

(zum Beispiel ein Tablet), geben Sie hier 0 ein. Geben Sie die Telefonnummer in internationalem Format an, zum Beispiel: "+491701234567".

e) Wenn Sie das Gerät per E-Mail provisionieren möchten, zum Beispiel ein Tablet, das keine Telefonnummer hat, geben Sie eine E-Mail-Adresse im **E-Mail-Adresse** Feld ein. Für weitere Informationen siehe *Konfigurieren der Provisionierung per E-Mail* (Seite 34).

f) Wählen Sie im **Eigentümer** Feld **Firmengerät** oder **Privates Gerät**.

5. Um einen LDAP-Link zum Gerät hinzuzufügen, klicken Sie auf die **LDAP-Verknüpfung setzen** Schaltfläche. Für weitere Informationen siehe *Hinzufügen einer LDAP-Verknüpfung zum Gerät* (Seite 97).
6. Um eigene Eigenschaften zum Gerät hinzuzufügen, wechseln Sie in die **Eigene Eigenschaften** Registerkarte und klicken Sie auf die **Neue Eigenschaft anlegen** Schaltfläche. Für weitere Informationen siehe *Definieren eigener Eigenschaften für Geräte* (Seite 97).
7. Wenn Sie alle erforderlichen Gerätedetails angegeben haben, klicken Sie auf die **Speichern** Schaltfläche.

Das neue Gerät wird zur Sophos Mobile Control Verwaltung hinzufügt und in der **Geräte** Ansicht unter **Inventar** angezeigt. Das Gerät wird auch bei der ausgewählten Gerätegruppe unter **Mitglieder** angezeigt. Sie können das Gerät nun provisionieren und verwalten.

14.3 Importieren von Geräten

Sie können neue Geräte durch Import einer .csv-Datei mit bis zu 500 Geräten hinzufügen. In der **Geräte importieren** Ansicht steht eine Musterdatei mit den korrekten Spaltennamen und der richtigen Spaltenreihenfolge zum Download zur Verfügung.

Hinweis: Verwenden Sie einen Text-Editor zum Bearbeiten der .csv-Datei. Wenn Sie Microsoft Excel verwenden, werden die eingegebenen Werte u. U. nicht korrekt aufgelöst. Speichern Sie die Datei mit der Dateinamenerweiterung .csv.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Geräte**.

   Die **Geräte** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Geräte importieren**.

   Es wird eine Meldung für die Auswahl der Datenquelle angezeigt.

3. Wählen Sie **CSV-Datei** aus der Dropdown-Liste und klicken Sie auf die **Ja** Schaltfläche.

   Die **Geräte importieren** Ansicht wird angezeigt.

   Hinweis: Wenn Sie noch keine .csv-Datei mit Geräten haben, können Sie nun eine Musterdatei herunterladen und diese zum Erstellen Ihrer Importdatei verwenden.

4. Wählen Sie die zu importierende .csv-Datei aus und klicken Sie auf **Datei hochladen**.

   Die Einträge in der .csv-Datei werden auf Fehler überprüft und auf der Import-Seite angezeigt.

   Hinweis: Wenn die .csv-Datei Fehler enthält, kann sie nicht importiert werden. Neben den relevanten Einträgen wird jeweils eine Fehlermeldung angezeigt. Bearbeiten Sie die .csv-Datei entsprechend und versuchen Sie es noch einmal.

5. Wenn alle Einträge korrekt sind, klicken Sie auf die **Fertigstellen** Schaltfläche.

Die in der .csv-Liste aufgelisteten Geräte werden importiert und in der **Geräte** Ansicht angezeigt. Die Geräte werden auch in der in der .csv-Datei angegebenen Gerätegruppe unter **Mitglieder** angezeigt. Sie können die Geräte nun provisionieren und verwalten.

14.4 Importieren von BlackBerry-Geräten über den BlackBerry Enterprise Server

BlackBerry-Geräte lassen sich über den BlackBerry Enterprise Server in Sophos Mobile Control importieren und in der **Geräte** Ansicht anzeigen.

Hinweis: BlackBerry-Geräte werden für Sophos Mobile Control as a Service nicht unterstützt.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Geräte**.

   Die **Geräte** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Geräte importieren**.

   Es wird eine Meldung für die Auswahl der Datenquelle angezeigt.

3. Wählen Sie **BlackBerry Enterprise Server** aus der Dropdown-Liste und klicken Sie auf die **Ja** Schaltfläche.

   Die **Geräte importieren** Ansicht wird angezeigt.

4. Klicken Sie auf die **Durchsuchen** Schaltfläche, um eine Liste aller beim BlackBerry Enterprise Server registrierten Geräte aufzurufen. Für diese Liste können Sie auch einen Filter über die Felder **Benutzername** und **E-Mail** definieren.
5. Wählen Sie die zu importierenden Geräte aus und klicken Sie auf die **Fertigstellen** Schaltfläche.

   Eine Meldung wird angezeigt.

6. Geben Sie in der Meldung an, ob alle oder nur ausgewählte Geräte importiert werden sollen. Geben Sie außerdem die zu verwendende Vorlage und Gerätegruppe an.
7. Klicken Sie auf die **Ja** Schaltfläche, um Ihre Auswahl zu bestätigen.

Die ausgewählten BlackBerry-Geräte werden importiert und in der **Geräte** Ansicht angezeigt.

Hinweis: Für BlackBerry-Geräte werden nur bestimmte Funktionen unterstützt: Anzeigen der Geräte in Sophos Mobile Control, Sperren, Zurücksetzen, Anzeigen des Software-Inventars, Anzeigen der Geräteeigenschaften. Das Self Service Portal unterstützt BlackBerry-Geräte nicht.

15 Provisionieren von Geräten über die Sophos Mobile Control Web-Konsole

Nachdem Sie die Geräte in der Web-Konsole hinzugefügt haben, müssen sie mit der Sophos Mobile Control Client-Komponente provisioniert werden. Die hierfür notwendigen Schritte richten sich nach dem Mobilgerätetyp:

- Android-Geräte und Windows Mobile Geräte werden durch Installation des SMC Client provisioniert.
- Apple iOS Geräte werden durch iOS MDM Client Bootstrap provisioniert.

Die Provisionierung wird in der Regel nur einmal pro Gerät ausgeführt.

Hinweis: Für Android- und iOS-Geräte ohne Telefonnummern, zum Beispiel Tablets, kann die Provisionierung über E-Mail erfolgen. Diese Provisionierungsmethode können Sie in der Web-Konsole konfigurieren, siehe *Konfigurieren der Provisionierung per E-Mail* (Seite 34). Diese Geräte können auch vom Endbenutzer über das Self Service Portal eingerichtet werden. Weitere Informationen finden Sie in den *Sophos Mobile Control Benutzerhandbüchern für Android und Apple iOS*.

Hinweis: Sie können alle Aufträge, die für die vollständige Registrierung und Provisionierung eines Geräts notwendig sind, bündeln, indem Sie Auftragspakete für die Provisionierung des Geräts, die Anwendung der erforderlichen Richtlinien und die Installation der erforderlichen Anwendungen (zum Beispiel Managed Apps für Apple iOS Geräte) erstellen. Für weitere Informationen siehe *Mit Auftragspaketen arbeiten* (Seite 78).

Hinweis: Geräte, die von Endbenutzern über das Self Service Portal registriert werden, können durch Angeben eines Auftragspakets für die Provisionierung bei der Konfiguration der Einstellungen für die Benutzung des Self Service Portal provisioniert werden. Weitere Informationen dazu, wie Sie die für die Provisionierung erforderlichen Auftragspakete erstellen, finden Sie in der *Sophos Mobile Control Startup-Anleitung* bzw. in der *Sophos Mobile Control as a Service Startup-Anleitung*. Für weitere Informationen zum Auswählen des Auftragspakets in den Self Service Portal Einstellungen siehe *Konfigurieren von Self Service Portal Einstellungen* (Seite 85). Weitere Informationen zur Benutzung des Self Service Portal finden Sie in den *Sophos Mobile Control Benutzerhandbüchern für Android, Apple iOS und Windows Mobile*.

15.1 Hinzufügen von Sophos Mobile Control Client-Paketen

Damit Sie Geräte provisionieren können, müssen die aktuellen Sophos Mobile Control Client Pakete in der Web-Konsole verfügbar sein. Neue Pakete lassen sich über von Sophos gelieferte Updates hinzufügen. Sie können neue Pakete auch wie folgt in der Web-Konsole hinzufügen:

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Ersteinrichtung** auf **SMC-Client Pakete**.

   Die **Sophos Mobile Control-Client Pakete** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neues Paket anlegen**.

   Die **Paket bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Version** für das neue Client-Paket ein.
4. Wählen Sie unter **Betriebssysteme** die kompatiblen Betriebssysteme für das neue Client-Paket.
5. Geben Sie an, wie das Client-Paket zur Verfügung gestellt wird:
   - Wählen Sie **Paket hochladen**, um das Paket direkt in die Web-Konsole hochzuladen. Wählen Sie das gewünschte Paket aus und klicken Sie auf **Übertragen**.
   - Um einen Link zum Client-Paket bereitzustellen, wählen Sie **Paket verlinken**. Geben Sie unter **Link** den relevanten Link an. Das **Link** Feld ist ein Pflichtfeld. Für Informationen dazu, wie Sie Links zu iOS- und Android-Client-Paketen erstellen, siehe *Erstellen von Links zu Paketen* (Seite 43).
6. Klicken Sie auf die **Speichern** Schaltfläche.

Das Sophos Mobile Control Client-Paket ist für die Ersteinrichtung verfügbar. Es wird in der **Sophos Mobile Control-Client Pakete** Ansicht angezeigt.

15.2 Provisionieren von Android-Geräten und Windows Mobile Geräten

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Ersteinrichtung** auf **SMC-Client Installation**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.
2. In dieser Ansicht haben Sie folgende Möglichkeiten:
   - Wählen Sie einzelne Geräte, die Sie provisionieren möchten.
   - Klicken Sie auf die **Gruppenauswahl** Schaltfläche, um die **Gerätegruppe(n) wählen** Ansicht zu öffnen. Wählen Sie dann ein oder mehrere Gerätegruppen für die Ersteinrichtung aus.
3. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Die **Software wählen** Ansicht wird angezeigt.
4. Wählen Sie das Sophos Mobile Control Client-Paket aus, dass Sie installieren möchten, und klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.
5. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
6. Wählen Sie die Option **Ausführung erzwingen**, um die Client-Installation für die ausgewählten Geräte zu erzwingen.
7. Klicken Sie auf die **Fertigstellen** Schaltfläche.

Bei den ausgewählten Geräten wird zum angegebenen Zeitpunkt die Ersteinrichtung ausgeführt. Nach dem erfolgreichen Abschluss dieses Vorgangs und der Synchronisierung mit dem Server, wird der Gerätestatus der Geräte mit **Managed** angegeben.

15.3 Provisionieren von iOS-Geräten

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Ersteinrichtung** auf **iOS MDM-Client Bootstrap**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

2. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Wählen Sie einzelne Geräte, die Sie provisionieren möchten.
   - Klicken Sie auf die **Gruppenauswahl** Schaltfläche, um die **Gerätegruppe(n) wählen** Ansicht zu öffnen. Wählen Sie dann ein oder mehrere Gerätegruppen für die Ersteinrichtung aus.

3. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

4. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
5. Wählen Sie die Option **Ausführung erzwingen**, um den iOS MDM Client Bootstrap für die ausgewählten Geräte zu erzwingen.

Bei den ausgewählten Geräten wird zum angegebenen Zeitpunkt der Bootstrap-Vorgang ausgeführt. Um die Ersteinrichtung abzuschließen, müssen Sie die Sophos Mobile Control App auf dem Gerät installieren, siehe *Installieren von Softwarepaketen* (Seite 46).

16 Mit Softwarepaketen und Applikationen arbeiten

In der Web-Konsole können Sie unter **Applikationen** Softwarepakete erstellen, die auf Geräten installiert werden sollen. Die Pakete können aus mehreren Dateien bestehen. Sie sind jedoch in der Regel als betriebssystemspezifische Datei gepackt (z. B. "cab", "apk" oder "ipa").

Wenn Sie Softwarepakete erstellen, können Sie die auf den Geräten zu installierenden Pakete wie folgt zur Verfügung stellen:

- Sie können das Paket in die Web-Konsole hochladen.
- Sie können einen Link für den Download zur Verfügung stellen.

Neben der Installation und Deinstallation von Softwarepaketen können Sie hier Prozesse auf Windows Mobile Geräten freischalten oder sperren.

16.1 Erstellen von Links zu Paketen

Wenn Sie Links zu Paketen bereitstellen möchten, müssen Sie diese vor dem Anlegen der Softwarepakete in der Web-Konsole erstellen. Die folgenden Abschnitte beschreiben, wie Sie einen Link zu Paketen für Apple iOS und Android erstellen.

16.1.1 Erstellen von Links zu iOS-Paketen

1. Gehen Sie in Ihrem Browser zu *http://itunes.apple.com/linkmaker*.
2. Geben Sie in den **Link Maker** Feldern Folgendes für die relevante App an:
   - Geben Sie im **Search** Feld einen Suchbegriff ein, zum Beispiel den App-Hersteller oder Teil des App-Namens.
   - **Country (Land)**
   - **Media Type (Medientyp)**
   - **Genre/Category (Genre/Kategorie)**
3. Klicken Sie auf **Search**.

   Die gefundenen Apps werden unter den Suchfeldern angezeigt.
4. Klicken Sie bei der gewünschten App auf **iPhone App Link** oder **iPad App Link**.

   Das Fenster **Linking to App:** wird angezeigt. Es zeigt den generierten Link.
5. Kopieren Sie den unter **Direct Link** angezeigten Link.

Sie können den generierten Link beim Erstellen eines Softwarepakets einfügen.

16.1.2 Erstellen von Links zu Android-Paketen

1. Gehen Sie in Ihrem Browser zu *https://play.google.com/store*.
2. Suchen Sie nach der erforderlichen App und öffnen Sie sie.

3. Kopieren Sie den Link in der Web-Adressenzeile Ihres Browsers.

Sie können diesen Link beim Erstellen eines Softwarepakets einfügen.

16.2 Erstellen von Softwarepaketen

1. Klicken Sie in der Web-Konsole unter **Applikationen** auf **Softwarepakete**.

   Die **Softwarepakete** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neues Paket anlegen**.

   Die **Paket bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Version** für das neue Softwarepaket ein. Diese beiden Felder sind Pflichtfelder.
4. Für Android-Geräte und Apple iOS-Geräte können Sie die Software über den Enterprise App Store zur Verfügung stellen und sie als empfohlen oder erforderlich definieren. Wählen Sie hierzu im **Empfehlungsstatus** Feld **Empfohlen** oder **Erforderlich**.
5. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das die Backup-Konfiguration gelten soll.
6. Geben Sie an, wie das Softwarepaket zur Verfügung gestellt wird:
   - Wählen Sie **Paket hochladen**, um das Paket direkt in die Web-Konsole hochzuladen. Wählen Sie das gewünschte Paket aus und klicken Sie auf **Übertragen**.
   - Um einen Link zum Client-Paket bereitzustellen, wählen Sie **Paket verlinken**. Geben Sie unter **Link** den relevanten Link an. Das **Link** Feld ist ein Pflichtfeld.
7. Klicken Sie auf die **Speichern** Schaltfläche.

Das Softwarepaket steht für die Installation zur Verfügung. Es wird in der **Softwarepakete** Ansicht angezeigt. Wenn Sie die Software als **Empfohlen** oder **Erforderlich** konfiguriert haben, wird sie im Enterprise App Store des Sophos Mobile Control Client auf dem Endbenutzergerät zum Download angezeigt. Die Benutzer können sie zur Installation auswählen. Der Installationsvorgang läuft ohne oder nur mit sehr geringer Benutzerinteraktion. Weitere Informationen zur Installation von erforderlichen oder empfohlenen Apps finden Sie in den *Sophos Mobile Control Benutzerhandbüchern für Android, Apple iOS und Windows Mobile*.

16.2.1 Herunterladen von Softwarepaketen aus der Web-Konsole

Wenn Sie das Software-Paket in das System hochgeladen haben, können Sie es jederzeit wieder herunterladen, um es zu überprüfen. So müssen Sie die Dateien nicht separat verwalten.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Applikationen** auf **Softwarepakete**.

   Die **Softwarepakete** Ansicht wird angezeigt.

2. Klicken Sie beim gewünschten Softwarepaket auf das **Bearbeiten** Bleistiftsymbol.

   Die **Paket bearbeiten** Ansicht wird angezeigt.

3. Klicken Sie auf das **Download** Symbol neben dem Softwarepaket.

   Ein Dialog für den Datei-Download wird angezeigt.

4. Speichern Sie die Datei am gewünschten Speicherort.

16.3 Verwaltung von mit dem Apple Volume Purchase Program erworbenen Apps

Mit dem Apple Volume Purchase Program (VPP) können Sie iOS Apps in großen Mengen kaufen und diese im Unternehmen verteilen. Detaillierte Informationen zur Registrierung und zur Benutzung des Apple Volume Purchase Program finden Sie unter *http://www.apple.com/business/vpp/*.

Wenn eine beim Apple Volume Purchase Programm aufgegebene Bestellung abgeschlossen ist, können Sie eine Excel-Tabelle mit Codes für die erworbenen Apps herunter laden. Zur Verwaltung der mit dem Apple Volume Purchase Program erworbenen Apps mit Sophos Mobile Control können Sie die Code-Tabelle hochladen und die einzelnen VPP-Codes den entsprechenden Softwarepaketen in der Sophos Mobile Control Web-Konsole zuweisen.

16.3.1 Hochladen und Zuweisen von VPP-Codes

Voraussetzungen:

- Sie haben die .xls-Tabelle mit den Codes für die erworbenen Apps bei Apple heruntergeladen. Weitere Informationen zur Benutzung des Apple Volume Purchase Program finden Sie unter *http://www.apple.com/business/vpp/*.
- Sie haben Softwarepakete mit Links zu den erworbenen iOS Apps in der Web-Konsole erstellt. Für weitere Informationen siehe *Erstellen von Links zu iOS-Paketen* (Seite 43) und *Erstellen von Softwarepaketen* (Seite 44).

1. Klicken Sie in der Web-Konsole unter **Applikationen** auf **Softwarepakete**.

   Die **Softwarepakete** Ansicht wird angezeigt.

2. Klicken Sie auf das **Bearbeiten** Bleistiftsymbol neben der gewünschten iOS App.

   Die **Paket bearbeiten** Ansicht wird angezeigt.

3. Klicken Sie auf die **Anzeigen** Schaltfläche neben dem **VPP-Codes** Feld.

   Die **VPP-Codes** Ansicht wird angezeigt.

4. Suchen Sie nach der .xls-Datei, die Sie heruntergeladen haben, und klicken Sie auf **Übertragen**.

   Die **VPP Codes** Ansicht wird mit den Code-Informationen aus der .xls-Datei aktualisiert.

   - Das **Verfügbare Codes** Feld zeigt die Anzahl an verfügbaren Codes.
   - Das **Reservierte Codes** Feld zeigt die Anzahl an Codes, die für spezifische Geräte reserviert sind.
   - Das **Verbrauchte Codes** Feld zeigt die Anzahl an verbrauchten Codes.
   - Das **Ungültige Codes** Feld zeigt die Anzahl an ungültigen Codes.

   In der Tabelle darunter werden die einzelnen Codes mit ihrem jeweiligen Status angezeigt. Wenn Codes für bestimmte Geräte reserviert sind, werden die UDIDs der Geräte angezeigt.

5. Wählen Sie den Code, den Sie der iOS App zuweisen möchten, und klicken Sie auf **Übernehmen**.

   Die **Paket bearbeiten** Ansicht wird wieder angezeigt.

6. Klicken Sie auf die **Speichern** Schaltfläche.

16.4 Installieren von Softwarepaketen

Voraussetzung: Das relevante Softwarepaket wurde unter **Applikationen** - **Softwarepakete** erstellt.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Applikationen** auf **Installation**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

2. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Wählen Sie einzelne Geräte aus, auf denen das Softwarepaket installiert werden soll.
   - Klicken Sie auf die **Gruppenauswahl** Schaltfläche, um die **Gerätegruppe(n) wählen** Ansicht zu öffnen. Wählen Sie dann ein oder mehrere Gerätegruppen für die Installation der Software aus.

3. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Die **Software wählen** Ansicht wird angezeigt.

4. Wählen Sie das Softwarepaket aus, dass Sie installieren möchten, und klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

5. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
6. Wählen Sie die Option **Ausführung erzwingen**, um die Installation für die ausgewählten Geräte zu erzwingen.
7. Wählen Sie **Anwendung freischalten**, um die Anwendung auf dem Gerät zu aktivieren.

8. Wählen Sie **Ohne Benutzerinteraktion** (sofern unterstützt), um das Software-Paket ohne Benutzerinteraktion zu installieren.

   Hinweis: Die Installation ohne Benutzerinteraktion wird unter Umständen nicht für alle Geräte unterstützt.

9. Klicken Sie auf die **Fertigstellen** Schaltfläche.

Das Softwarepaket wird zum angegebenen Zeitpunkt auf den ausgewählten Geräten installiert.

16.5 Deinstallieren von Softwarepaketen

Hinweis: Die stille Deinstallation funktioniert bei iOS-Geräten für Managed Apps, die über Sophos Mobile Control verteilt wurden, und bei Windows Mobile Geräten. Bei Android-Geräten ist eine stille Deinstallation nicht möglich.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Applikationen** auf **Deinstallation**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

2. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Wählen Sie einzelne Geräte für die Deinstallation der Software aus.
   - Klicken Sie auf die **Gruppenauswahl** Schaltfläche, um die **Gerätegruppe(n) wählen** Ansicht zu öffnen. Wählen Sie dann ein oder mehrere Gerätegruppen für die Deinstallation der Software aus.

3. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Die **Software wählen** Ansicht wird angezeigt. Sie zeigt alle auf den ausgewählten Geräten installierten Anwendungen.

4. Wählen Sie die Anwendung(en), die Sie deinstallieren möchten, und klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

5. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
6. Wählen Sie die Option **Ausführung erzwingen**, um die Deinstallation für die ausgewählten Geräte zu erzwingen.
7. Klicken Sie auf die **Fertigstellen** Schaltfläche.

Die ausgewählten Anwendungen werden zum angegebenen Zeitpunkt auf den ausgewählten Geräten deinstalliert.

16.6 Anwenden des Softwarefilters

Mit Filtern lässt sich die Anzahl an in Listen angezeigten Einträgen nach definierten Kriterien einschränken. Mit dem Softwarefilter lassen sich die angezeigten Ergebnisse in Listen mit Softwarepaketen einschränken.

Hinweis: Die Filter gelten nicht nur für die derzeit angezeigte Funktion, sondern für alle Funktionen, bei denen Einträge dieses Typs aufgelistet werden.

So wenden Sie den Softwarefilter an:

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Applikationen** auf **Softwarepakete**.

   Die **Softwarepakete** Ansicht wird angezeigt.

2. Klicken Sie auf die **Filter** Schaltfläche (Lupensymbol) im Header der Web-Konsole.

   Der **Softwarefilter** Dialog wird mit dem Status **Es ist kein Filter aktiv** angezeigt.

3. Im **Softwarefilter** Dialog können Sie die folgenden Filteroptionen auswählen:

Option	Beschreibung
Name	Nach Paketname filtern.
Version	Nach Paketversion filtern.
Betriebssystem	Nach Betriebssystemen filtern, für die die Pakete anwendbar sind.

4. Wenn Sie die erforderlichen Kriterien ausgewählt haben, klicken Sie auf **Filtern**.

Der Filter wird aktiviert und die Geräteliste wird neu geladen. Die **Filter** Schaltfläche im Header der Web-Konsole ändert ihre Farbe von Blau zu Pink. Daduch wird angezeigt, dass der Filter aktiv ist. Für das Zurücksetzen des Filters wird im Header die **Aufheben** Schaltfläche angezeigt. Der Status des Softwarefilters im **Softwarefilter** Dialog ändert sich zu **Es ist ein Filter aktiv**.

Hinweis: Denken Sie daran, Filter manuell wieder aufzuheben, wenn sie nicht mehr benötigt werden. Andernfalls enthalten Listen oder Berichte unter Umständen nicht die erwarteten Ergebnisse.

16.7 Freischalten/Sperren von Prozessen auf Windows Mobile Geräten

In der Web-Konsole können Sie unter **Applikationen** Prozesse auf Windows Mobile Geräten freischalten oder sperren. Gesperrte Prozesse dürfen nicht ausgeführt werden. Der Sophos Mobile Control Client überwacht alle Prozesse, die auf einem Gerät laufen, und bricht gesperrte Prozesse sofort ab. Somit können Sie als Administrator bestimmte Applikationen sperren. Freigeschaltete Prozesse sind nicht betroffen und können gestartet werden.

Hinweis: Wenn auf dem Gerät Softwarepakete manuell installiert werden (nicht über Sophos Mobile Control), so werden die enthaltenen Prozesse standardmäßig gesperrt. Wird das Paket über Sophos Mobile Control installiert, werden die Prozesse automatisch aktiviert.

Hinweis: Wenn ein Paket, das aktivierte Prozesse enthält, deinstalliert wird, bleiben die Prozesse aktiviert. Wird diese Applikation wieder installiert, so sind die Prozesse noch aktiviert. Dabei spielt es keine Rolle, ob die Installation über Sophos Mobile Control oder manuell erfolgt.

Prozesse lassen sich für einzelne oder mehrere Geräte freischalten oder sperren.

Hinweis: Für Windows Mobile Control Geräte ist das Freischalten und Sperren von Prozessen standardmäßig deaktiviert. Sie können diese Funktionalität mit dem setConfig Befehl (ProcessSecurityOn) aktivieren.

16.7.1 Freischalten/Sperren von Prozessen auf einzelnen Geräten

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Applikationen** auf **Sperren/Freischalten**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

2. Wählen Sie das gewünschte Gerät aus und klicken Sie auf **Weiter**.

   Die **Prozesse freischalten/sperren** Ansicht wird angezeigt.

3. Wählen Sie in den beiden angezeigten Tabellen die gewünschten Softwarepakete und Systemprozesse aus und schalten Sie diese frei oder sperren Sie sie, indem Sie auf die entsprechenden Symbole klicken.
4. Klicken Sie auf **Next**.

   Die **Ausführungszeit und Beschreibung wählen** Ansicht wird angezeigt.

5. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
6. Ändern Sie im **Beschreibung** Feld die angezeigte Beschreibung, falls notwendig.
7. Klicken Sie auf die **Fertigstellen** Schaltfläche.

Die ausgewählten Prozesse werden auf dem gewählten Gerät zum angegebenen Zeitpunkt freigeschaltet/gesperrt.

16.7.2 Freischalten/Sperren von Prozessen auf mehreren Geräten

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Applikationen** auf **Sperren/Freischalten**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

2. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Wählen Sie mehrere einzelne Geräte aus.
   - Klicken Sie auf die **Gruppenauswahl** Schaltfläche, um die **Gerätegruppe(n) wählen** Ansicht zu öffnen und wählen Sie Gerätegruppen aus.

3. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Die **Gerät für Datenbasis wählen** Ansicht wird angezeigt.

4. Wählen Sie das Gerät aus, dass Sie als Datenquelle für Softwarepakete und Systemprozesse verwenden möchten, indem Sie auf das Pfeilsymbol neben dem gewünschten Gerät klicken. Das ausgewählte Gerät dient als Grundlage für die Prozessinformationen. Es werden nur die Prozesse für dieses Gerät zur Aktivierung/Deaktivierung angezeigt. Es sind jedoch alle Geräte, die in der **Gerät(e) wählen** oder **Gerätegruppe(n) wählen** Ansicht ausgewählt wurden, von dem Sperren/Freischalten-Prozess betroffen, wenn Sie dieselben Systemprozesse haben.

   Die **Prozesse freischalten/sperren** Ansicht wird angezeigt.

5. Wählen Sie in den beiden angezeigten Tabellen die gewünschten Softwarepakete und Systemprozesse aus und schalten Sie diese frei oder sperren Sie sie, indem Sie auf die entsprechenden Symbole klicken.
6. Klicken Sie auf **Next**.

   Die **Ausführungszeit und Beschreibung wählen** Ansicht wird angezeigt.

7. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
8. Ändern Sie im **Beschreibung** Feld die angezeigte Beschreibung, falls notwendig.
9. Klicken Sie auf die **Fertigstellen** Schaltfläche.

Die ausgewählten Prozesse werden auf den gewählten Geräten zum angegebenen Zeitpunkt freigeschaltet/gesperrt.

17 Mit Konfigurationen (Profilen) arbeiten

In der Web-Konsole können Sie unter **Konfigurationen** Einstellungsprofile für iOS-, Android- und Windows Mobile Geräte erstellen und übertragen.

Für iOS-Geräte können Sie auch Profile hochladen, die mit der iPhone Configuration Utility erstellt wurden, und diese an Geräte übertragen.

Für Windows Mobile Geräte können Sie Vorlagen für Einstellungsprofile verwalten. Sie definieren die Einstellungsoptionen, die für die Benutzer der Web-Konsole zur Verfügung stehen. Die Vorlagen werden von Sophos zur Verfügung gestellt.

Hinweis: Für Android-Geräte richten sich die unterstützten Einstellungen nach herstellerspezifischen APIs. Je nach Endbenutzergerät haben einige Einstellungen unter Umständen keine Auswirkungen. Weitere Informationen finden Sie in der Feature Matrix im *Sophos Mobile Control Technical Guide* (Englisch).

17.1 Erstellen von Profilen für iOS-Geräte

Für das Erstellen von Profilen für iOS-Geräte bietet Sophos Mobile Control zwei Verfahren:

- Sie können iOS-Profile direkt in der Web-Konsole anlegen.
- Sie können mit der Apple iPhone Configuratoin Utility erstellte Profile in die Web-Konsole importieren.

17.1.1 Erstellen von iOS-Profilen in der Web-Konsole

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Konfigurationen** - **Apple iOS** auf **Profile**.

   Die **Profile** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neues Profil anlegen**.

   Die **Profil bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Version** für das neue Profil ein.
4. Geben Sie im **Kennung** Feld eine eindeutige Kennung für das Profil ein.

   Hinweis: Sonderzeichen, zum Beispiel ä, ö oder Leerzeichen, werden in Kennungen für iOS-Profile nicht unterstützt.

5. Geben Sie im **Organisation** Feld den Namen der Organisation für das Profil ein, zum Beispiel einen Firmennamen.
6. Geben Sie im Feld **Beschreibung** eine Beschreibung für das Profil ein.
7. Legen Sie im **Durch Benutzer entfernbar** Feld fest, ob Benutzer das Profil von ihrem Gerät entfernen dürfen:

   - **Immer**

- **Mit Authentifizierung**

  Wenn Sie diese Option auswählen, wird unter dem **Durch Benutzer entfernbar** Feld das Feld **Kennwort für Authentisierung** angezeigt. Geben Sie das für das Entfernen des Profils erforderliche Kennwort ein. Um Benutzern zu ermöglichen, das Profil zu entfernen, teilen Sie ihnen das Kennwort mit.

- **Nie**

8. Im **Automatisch entfernen am** Feld können Sie ein Datum angeben, an dem das Profil automatisch von Endbenutzergeräten entfernt wird. Das Profil wird am festgelegten Datum um 23:00 entfernt.
9. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das das Profil gelten soll.

   Hinweis: Das **Betriebssysteme** Feld zeigt alle iOS-Versionen, die derzeit im System verfügbar sind. Für die einzelnen iOS-Versionen werden u. U. nicht alle Konfigurationseinstellungen unterstützt. Wenn Sie unter **Betriebssysteme** alle Versionen auswählen, haben je nach iOS-Version auf dem Endbenutzergerät einige Einstellungen u. U. keinerlei Auswirkungen.

10. Klicken Sie auf die **Hinzufügen** Schaltfläche, um Konfigurationen mit iPhone-Konfigurationseinstellungen zum Profil hinzuzufügen.

    Die **Verfügbare Konfigurationen** Ansicht wird angezeigt.

11. Wählen Sie die Konfiguration aus, die Sie hinzufügen möchten, und klicken Sie auf **Weiter**.

    Die Einstellungen-Ansicht der Konfiguration wird angezeigt.

12. Definieren Sie die erforderlichen Einstellungen. Für eine detaillierte Liste aller verfügbaren Konfigurationen und Einstellungen siehe *Verfügbare iOS-Konfigurationen* (Seite 52).
13. Klicken Sie auf die **Übernehmen** Schaltfläche, um Ihre Änderungen zu speichern.

    Die Konfiguration wird in der **Profil bearbeiten** Ansicht unter **Konfigurationen** angezeigt.

14. Fügen Sie nach Wunsch weitere Konfigurationen hinzu.
15. Wenn Sie alle erforderlichen Konfigurationen hinzugefügt haben, klicken Sie auf die **Speichern** Schaltfläche.

Das Profil steht für die Übertragung zur Verfügung. Es wird in der **Profile** Ansicht angezeigt.

17.1.2 Verfügbare iOS-Konfigurationen

Die folgenden Konfigurationen sind für iOS-Profile in der **Verfügbare Konfigurationen** Ansicht verfügbar, wenn Sie ein Profil erstellen oder bearbeiten. Einige Konfigurationen lassen sich in einem Profil nur einmal hinzufügen, andere mehrmals.

Hinweis: Die unterstützten Einstellungen hängen von der iOS-Version ab, die auf den einzelnen Geräten in Gebrauch ist. Je nach Endbenutzergerät haben einige Einstellungen unter Umständen keine Auswirkungen. Weitere Informationen finden Sie in der Feature Matrix im *Sophos Mobile Control Technical Guide* (Englisch).

Kennwortrichtlinien

In dieser Konfiguration können Sie Kennwortrichtlinien für Geräte definieren. Sie können nur eine **Kennwortrichtlinien** Konfiguration in einem Profil hinzufügen.

Einstellung/Feld	Beschreibung
Einfache Werte erlauben	Wenn Sie diese Option auswählen, dürfen Benutzer aufeinander folgende oder wiederholte Zeichen in ihrem Kennwort verwenden, zum Beispiel "1111" oder "abcde".
Alphanumerische Werte erforderlich	Wenn Sie diese Option auswählen, müssen Kennwörter mindestens einen Buchstaben oder eine Zahl enthalten.
Mindestlänge des Kennworts	Gibt an, wie viele Zeichen ein Kennwort mindestens enthalten muss.
Mindestanzahl von komplexen Zeichen	Gibt an, wie viele nicht-alphanumerische Zeichen (zum Beispiel & oder !) ein Kennwort mindestens enthalten muss.
Maximale Kennwortgültigkeit (1 - 730 Tage oder ohne)	Fordert eine Änderung des Kennworts im angegebenen Intervall. Wertebereich: 0 (keine Kennwortänderung erforderlich) bis 730 Tage.
Automatische Sperre (Minuten)	In diesem Feld können Sie festlegen, wann (in Minuten) das Gerät nach Nichtbenutzung gesperrt werden soll. Diese Einstellung legt den Höchstwert fest, den der Benutzer auf dem Gerät konfigurieren darf.
Anzahl der letzten Kennwörter, die nicht benutzt werden dürfen (1 - 50 oder ohne)	In diesem Feld können Sie festlegen, wie viele alte Kennwörter gespeichert und mit neu definierten Kennwörtern verglichen werden. Wenn ein Benutzer ein neues Kennwort festlegt, wird es nicht akzeptiert, wenn es mit einem bereits benutzten Kennwort übereinstimmt. Wertebereich: 1 bis 50 oder 0 (keine Kennworthistorie).
Zeitgrenze für Gerätesperrung	In diesem Feld können Sie festlegen, wie lang ein Gerät nach einer Sperre ohne Kennwort-Eingabeaufforderung entsperrt werden darf. Diese Einstellung legt den Höchstwert fest, den der Benutzer auf dem Gerät konfigurieren darf. Wenn Sie **Ohne**

Einstellung/Feld	Beschreibung
	auswählen, kann der Benutzer einen beliebigen verfügbaren Zeitraum wählen. Wenn Sie **Sofort** auswählen, müssen Benutzer immer, wenn Sie ihre Geräte entsperren, ein Kennwort eingeben.
Maximale Anzahl fehlerhafter Loginversuche	In diesem Feld können Sie die Höchstanzahl an fehlgeschlagenen Eingabeversuchen für das Kennwort eingeben. Nach Erreichen der Höchstanzahl wird das Gerät zurückgesetzt. Nach sechs fehlgeschlagenen Versuchen wird eine Zeitverzögerung verhängt. Ein erneuter Versuch kann erst nach Ablauf der Verzögerung unternommen werden. Diese Verzögerung wird mit jedem fehlgeschlagenen Versuch größer. Nach dem letzten fehlgeschlagenen Versuch werden alle Daten und Einstellungen sicher vom Gerät entfernt. Die Zeitverzögerung startet nach dem sechsten Versuch. Wenn Sie also diesen Wert auf **6** oder einen niedrigeren Wert setzen, wird keine Verzögerung ausgelöst. In diesem Fall wird das Gerät zurückgesetzt, sobald die maximale Anzahl an Fehlversuchen überschritten ist.

Einschränkungen

In dieser Konfiguration können Sie Einschränkungen für Geräte definieren. Sie können nur eine **Einschränkungen** Konfiguration in einem Profil hinzufügen.

Einstellung/Feld	Beschreibung
Gerätefunktionalität	
Installation von Programmen erlauben	Wenn Sie diese Option deaktivieren, wird der App Store deaktiviert und sein Symbol wird vom Home-Bildschirm entfernt. Benutzer können keine Apps über den App Store oder iTunes installieren oder aktualisieren.
Verwendung der Kamera erlauben	Wenn Sie diese Option deaktivieren, werden Kameras vollständig deaktiviert. Das Kamera-Symbol wird vom Home-Bildschirm entfernt. Benutzer können weder Fotos

Einstellung/Feld	Beschreibung
	machen, Videos aufzeichnen noch FaceTime benutzen.
FaceTime erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine FaceTime Anrufe tätigen oder erhalten.
Screenshot erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Screenshots vom Display erstellen.
Automatische Synchronisierung beim Roaming erlauben	Wenn Sie diese Option deaktivieren, synchronisieren sich Geräte beim Roaming nur dann, wenn der Benutzer auf ein Konto zugreift.
Siri erlauben	Wenn Sie diese Option deaktivieren, können Benutzer Siri, Sprachbefehle oder die Diktierfunktion nicht verwenden.
Siri erlauben während das Gerät gesperrt ist	Wenn Sie diese Option deaktivieren, müssen Benutzer ihre Geräte durch Eingabe ihres Kennworts entsperren, damit sie Siri benutzen können.
Sprachwahl erlauben	Wenn Sie diese Option deaktivieren, können Benutzer nicht mit Sprachwahl auf ihrem Telefon wählen.
Passbook bei Gerätesperre erlauben	Wenn Sie diese Option deaktivieren, zeigt das Gerät keine Passbook-Benachrichtigungen, wenn es gesperrt ist.
App-interne Käufe erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine App-internen Käufe durchführen.
Benutzer muss für alle Einkäufe das iTunes Store-Kennwort eingeben	Wenn Sie diese Option auswählen, müssen Benutzer für jeden Einkauf ihr Apple ID Kennwort eingeben. In der Regel gilt nach einem Einkauf eine kurze Wartezeit, bevor sich Benutzer für weitere Einkäufe erneut anmelden müssen.
Mehrspielermodus erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Spiele im Mehrspielermodus im Game Center spielen.

Einstellung/Feld	Beschreibung
Hinzufügen von Game Center-Freunden zulassen	Wenn Sie diese Option deaktivieren, können Benutzer keine Freunde im Game Center hinzufügen.
Programme	
Verwendung von YouTube erlauben	Wenn Sie diese Option deaktivieren, wird YouTube deaktiviert. Das YouTube-Symbol wird vom Home-Bildschirm entfernt.
iTunes Store darf verwendet werden	Wenn Sie diese Option deaktivieren, wird der iTunes Store deaktiviert und sein Symbol wird vom Home-Bildschirm entfernt. Benutzer können Inhalte weder in der Vorschau ansehen, noch kaufen oder herunterladen.
Verwendung von Safari erlauben	Wenn Sie diese Option deaktivieren, wird der Safari Web Browser deaktiviert und sein Symbol wird vom Home-Bildschirm entfernt. Dies verhindert auch, dass Benutzer Webclips öffnen.
Automatisches Ausfüllen aktivieren	Wenn Sie diese Option deaktivieren, werden Benutzereingaben in Webformularen von Safari nicht wiedererkannt.
Betrugswarnung erzwingen	Wenn Sie diese Option auswählen, verhindert Safari, dass Benutzer als betrügerisch oder schädlich erkannte Websites aufrufen.
JavaScript aktivieren	Wenn Sie diese Option deaktivieren, ignoriert Safari JavaScript auf Websites.
Pop-Ups unterdrücken	Wenn Sie diese Option auswählen, unterdrückt Safari Popups.
Cookies akzeptieren	In diesem Feld können Sie festlegen, ob Cookies akzeptiert werden sollen: ■ Immer ■ Nie ■ Von besuchten Webseiten
iCloud	

Einstellung/Feld	Beschreibung
Backup erlauben	Wenn Sie diese Option auswählen, können Benutzer ihre Geräte im iCloud-Speicher sichern.
Dokumentsynchronisierung erlauben	Wenn Sie diese Option auswählen, können Benutzer ihre Dokumente im iCloud-Speicher sichern.
Fotostream zulassen	Wenn Sie diese Option auswählen, können Benutzer Fotostreaming aktivieren. **Hinweis:** Wenn Sie ein Konfigurationsprofil installieren, dass die Benutzung von Fotostream einschränkt, werden Fotostream-Fotos vom Gerät des Benutzers entfernt. Es ist außerdem nicht möglich, Fotos aus dem Fotoordner an Fotostream zu senden. Wenn keine anderen Kopien dieser Fotos existieren, gehen diese u. U. verloren.
Freigegebene Fotostreams erlauben	Wenn Sie diese Option auswählen, können Benutzer andere einladen, ihre Fotostreams anzusehen. Außerdem können in diesem Fall Benutzer die freigegebenen Fotostreams anderer ansehen.
Sicherheit und Privatsphäre	
Senden von Diagnosedaten an Apple erlauben	Wenn Sie diese Option deaktivieren, werden keine iOS-Diagnosedaten an Apple gesendet.
Annehmen nicht vertrauenswürdiger TLS-Zertifikate durch Benutzer	Wenn Sie diese Option deaktivieren, werden Benutzer nicht gefragt, ob sie einem Zertifikat vertrauen möchten, das nicht verifiziert werden kann. Diese Einstellung gilt für Safari und Mail-Kontakte und Kalender-Accounts.
Verschlüsselte Backups erzwingen	Wenn Sie diese Option auswählen, müssen Backups verschlüsselt werden. Dies wird von iTunes für alle verschlüsselten Profile erzwungen.
Inhaltsbewertung	
Anstößige Musik und Podcasts erlauben	Wenn Sie diese Option deaktivieren, werden anstößiger Musik- oder Video-Inhalte im iTunes Store nicht angezeigt. Anstößige Inhalte werden von den jeweiligen Anbietern, zum Beispiel Plattenfirmen, bei der

Einstellung/Feld	Beschreibung
	Auflistung im iTunes Store entsprechend gekennzeichnet.

Exchange-ActiveSync

In dieser Konfiguration können Sie die Einstellungen für Ihren Microsoft Exchange Server definieren. Sie können mehrere **Exchange-ActiveSync** Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
Accountname	Geben Sie in diesem Feld den Accountnamen für das Exchange-ActiveSync Account ein.
Exchange-ActiveSync-Host	Geben Sie in diesem Feld den Microsoft Exchange Server ein.
Bewegen zulassen	Wenn Sie diese Option deaktivieren, können Benutzer ihre mit diesem Account gesendeten oder erhaltenen Nachrichten nicht in ein anderes Mail Account übertragen. Dies verhindert auch, dass Benutzer ein anderes Account für das Antworten auf oder das Weiterleiten von Nachrichten aus diesem Account verwenden.
Synchronisierung letzter Adressen erlauben	Wenn Sie diese Option deaktivieren, werden kürzlich verwendete Adressen nicht mit anderen Geräten über iCloud synchronisiert.
Nur mit Mail verwenden	Wenn Sie diese Option auswählen, kann dieses Account nur zum Senden von Mail-Nachrichten verwendet werden. Es kann nicht als Absender-Account für mit anderen Apps erstellten Nachrichten (zum Beispiel Fotos oder Safari) verwendet werden.
SSL	Wählen Sie diese Option, um für die gesamte Kommunikation SSL (Secure Socket Layer) zu verwenden.
Domain	Geben Sie in diesem Feld die Domäne für das Account an. Wenn Sie dieses Feld und das **Benutzer** Feld leer belassen, wird für den Benutzer eine Eingabeaufforderung auf dem Gerät angezeigt.

Einstellung/Feld	Beschreibung
Benutzer	Geben Sie in diesem Feld den Benutzer für das Account an. Wenn Sie dieses Feld und das **Domain** Feld leer belassen, wird für den Benutzer eine Eingabeaufforderung auf dem Gerät angezeigt.
E-Mail-Adresse	Geben Sie in diesem Feld die E-Mail-Adresse für das Account an.
Kennwort	Geben Sie in diesem Feld das Kennwort für das Account an.
Zeitraum für die Synchronisierung von E-Mails	Wählen Sie in diesem Feld den Zeitraum für die E-Mail-Synchronisierung. Dabei handelt es sich um die Anzahl an Tagen, für die E-Mails synchronisiert werden. Wenn Sie hier einen Zeitraum angeben, werden nicht alle im Posteingang enthaltenen E-Mails auf dem Mobilgerät synchronisiert, sondern nur die E-Mails aus dem angegebenen Zeitraum. Sie können folgende Optionen auswählen: ■ **Unbegrenzt** ■ **Ein Tag** ■ **Drei Tage** ■ **Eine Woche** ■ **Zwei Wochen** ■ **Ein Monat**
Identitätszertifikat	Wählen Sie in diesem Feld das Identitätszertifikat für die Verbindung zu ActiveSync. Wenn kein Zertifikat zur Auswahl verfügbar ist, wird eine Meldung angezeigt.

WiFi

In dieser Konfiguration geben Sie die Einstellungen für die Verbindung mit WiFi-Netzwerken an. Sie können mehrere **WiFi** Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
SSID	Geben Sie in diesem Feld die ID des Drahtlosnetzwerks an.

Einstellung/Feld	Beschreibung
Automatisch verbinden	Wählen Sie diese Option, um automatisch eine Verbindung mit dem Zielnetzwerk herzustellen.
Unsichtbares Netzwerk	Wählen Sie diese Option, wenn das Zielnetzwerk nicht offen oder unsichtbar ist.
Sicherheitstyp	In diesem Feld wählen Sie den Sicherheitstyp des WiFi-Netzwerks: ■ **Ohne** ■ **WEP** ■ **WPA/WPA2** ■ **Beliebig (persönlich)** ■ **Firmenweiter WEP** ■ **Firmenweiter WPA/WPA2** ■ **Beliebig (firmenweit)** Wenn Sie die persönlichen Einstellungen **WEP**, **WPA/WPA2** oder **Beliebig (persönlich)** wählen, wird ein **Kennwort** Feld angezeigt. Geben Sie das relevante Kennwort ein. Wenn Sie die firmenweiten Einstellungen **Firmenweiter WEP**, **Firmenweiter WPA/WPA2** oder **Beliebig (firmenweit)** wählen, werden die Registerkarten **Protokolle** und **Authentifizierung** angezeigt. Konfigurieren Sie in der **Protokolle** Registerkarte folgende Einstellungen: ■ Geben Sie unter **Akzeptierte EAP-Typen** die EAP-Verfahren an, die für die Authentisierung verwendet werden sollen. Je nach den hier ausgewählten Typen, lassen sich die Werte im Feld **Innere Identität (TTLS)** auswählen. ■ Konfigurieren Sie unter **EAP-FAST**, die Einstellungen für die EAP-FAST Protected Access Anmeldedaten.

Einstellung/Feld	Beschreibung
	In der **Authentifizierung** Registerkarte legen Sie die Einstellung für die Authentisierung fest: ■ Geben Sie im **Benutzer** Feld den Benutzernamen für die Verbindung zum Drahtlosnetzwerk ein. ■ Wählen Sie **Kennwort bei jedem Verbinden abfragen**, wenn das Kennwort für jede Verbindung abgefragt und mit der Authentisierung übertragen werden soll. ■ Geben Sie im **Kennwort** Feld das relevante Kennwort ein. ■ Wählen Sie im **Identitätszertifikat** Feld das Zertifikat für die Verbindung zum Drahtlosnetzwerk aus. ■ Geben Sie im **Externe Identität** Feld, die extern sichtbare ID (für TTLS, PEAP und EAP Fast) ein.
Proxy	Wählen Sie in diesem Feld die Proxy-Einstellungen für die WiFi-Verbindung: ■ **Ohne** ■ **Manuell** ■ **Automatisch** Wenn Sie **Manuell** auswählen, werden die Felder **Server und Port**, **Authentifizierung** und **Kennwort** angezeigt. Geben Sie die erforderlichen Proxy-Informationen ein. Wenn Sie **Automatisch** auswählen, wird das Feld **Proxy-Server-URL** angezeigt. Geben Sie die URL des Proxy-Servers ein.

VPN

In dieser Konfiguration können Sie VPN-Einstellungen für Netzwerke definieren. Sie können mehrere **VPN** Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
Verbindungsname	Geben Sie in diesem Feld den Namen der Verbindung ein, der auf dem Gerät angezeigt wird.
Verbindungstyp	Wählen Sie in diesem Feld den Verbindungstyp: ■ **Cisco AnyConnect** ■ **IPSec (Cisco)** Je nach hier gewähltem Verbindungstyp werden in der **VPN** Ansicht unterschiedliche Eingabefelder angezeigt.
Server (beide Verbindungstypen)	Geben Sie in diesem Feld den Host-Namen oder die IP-Adresse des Servers ein.
Account (beide Verbindungstypen)	Geben Sie in diesem Feld das Benutzer-Account für die Authentisierung der Verbindung ein.
Gruppe (Verbindungstyp **Cisco AnyConnect**)	Geben Sie in diesem Feld die Gruppe ein, die für die Authentisierung der Verbindung eforderlich sein kann.
Benutzer-Authentifizierung (Verbindungstyp **Cisco AnyConnect**)	Wählen Sie in diesem Feld die Art der Benutzer-Authentisierung: ■ **Kennwort** Wenn Sie diese Option auswählen, wird unter dem **Benutzer-Authentifizierung** Feld ein **Kennwort** Feld angezeigt. Geben Sie das Kennwort für die Authentisierung ein. ■ **Zertifikat** Wenn Sie diese Option auswählen, wird unter dem **Benutzer-Authentifizierung** Feld ein **Zertifikat** Feld angezeigt. Wählen Sie ein Zertifikat aus.
Geräte-Authentifizierung (Verbindungstyp **IPSec (Cisco)**)	Wählen Sie in diesem Feld die Art der Geräte-Authentisierung: ■ **Schlüssel (Shared Secret)/Gruppenname** Wenn Sie diese Option auswählen, werden die Felder **Gruppenname**, **Schlüssel (Shared Secret)**,

Einstellung/Feld	Beschreibung
	Hybrid-Authentifizierung verwenden und **Kennwort verlangen** unter dem **Geräte-Authentifizierung** Feld angezeigt. Geben Sie die erforderlichen Authentisierungsinformationen in den Feldern **Gruppenname** und **Schlüssel** (**Shared Secret**) ein. Wählen Sie je nach Anforderung **Hybrid-Authentifizierung verwenden** und **Kennwort verlangen**. ■ **Zertifikat** Wenn Sie diese Option auswählen, werden die Felder **Zertifikat** und **Inklusive Benutzer-PIN** unter dem **Geräte-Authentifizierung** Feld angezeigt. Wählen Sie im **Zertifikat** Feld das erforderliche Zertifikat aus. Wählen Sie **Inklusive Benutzer-PIN**, um die Benutzer-PIN in die Geräteauthentisierung einzubeziehen.
Proxy (beide Verbindungstypen)	Wählen Sie in diesem Feld die Proxy-Einstellungen für die Verbindung: ■ **Ohne** ■ **Manuell** Wenn Sie diese Option wählen, werden die Felder **Server und Port**, **Authentifizierung** und **Kennwort** angezeigt. Geben Sie im **Server und Port** Feld die gültige Adresse und den Port des Proxy-Servers ein. Geben Sie im **Authentifizierung** Feld den Benutzernamen für die Verbindung zum Proxy-Server ein. Geben Sie im **Kennwort** Feld das Kennwort für die Verbindung zum Proxy-Server ein. ■ **Automatisch** Wenn Sie diese Option wählen, wird das Feld **Proxy-Server-URL** angezeigt. Geben Sie die URL des Servers mit der Proxy-Einstellung in diesem Feld ein.

Webclip

In dieser Konfiguration können Sie Webclips definieren, die zum Home-Bildschirm der Benutzergeräte hinzugefügt werden. Webclips bieten schnellen Zugriff auf favorisierte Webseiten. Sie können jedoch zum Beispiel auch einen Webclip mit einer Support-Telefonnummer hinzufügen, damit die Benutzer schnell den Helpdesk kontaktieren können. Sie können mehrere **Webclip** Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
Beschreibung	Geben Sie in diesem Feld eine Beschreibung für den Webclip ein.
URL	Geben Sie in diesem Feld die URL für den Webclip ein.
Kann entfernt werden	Wenn Sie diese Option deaktivieren, kann der Benutzer den Webclip nicht entfernen. Der Webclip kann nur durch Entfernen des Profils, das den Webclip installiert hat, entfernt werden.
Bildschirmfüllend	Wenn Sie diese Option auswählen, wird der Webclip auf dem Gerät bildschirmfüllend geöffnet. Ein bildschirmfüllender Webclip öffnet die URL als Web App.

APN

Mit dieser Konfiguration können Sie den Name des Zugangspunkts (APN) des Geräts und die Mobilnetzwerk-Proxy-Einstellungen ändern. Diese Einstellungen legen fest, wie sich Geräte mit dem Netzwerk des Anbieters verbinden. Sie können nur eine **APN** Konfiguration in einem Profil hinzufügen.

Hinweis: Wenn diese Einstellungen nicht korrekt sind, kann das Gerät nicht auf Daten über ein Mobilnetzwerk zugreifen. Wenn Sie die Einstellungsänderungen rückgängig machen wollen, müssen Sie das Profil vom Gerät entfernen.

Einstellung/Feld	Beschreibung
Name des Zugangspunkts (APN)	Geben Sie in diesem Feld den Namen des Zugangspunkts des Anbieters (GPRS) ein.
Benutzername für Zugangspunkt	Geben Sie in diesem Feld den Benutzernamen für den Zugangspunkt ein. **Hinweis:** iOS unterstützt Benutzernamen für Zugangspunkte mit bis zu 64 Zeichen.

Einstellung/Feld	Beschreibung
Kennwort für Zugangspunkt	Geben Sie in diesem Feld das Kennwort für den Zugangspunkt ein. **Hinweis:** iOS unterstützt Kennwörter für Zugangspunkte mit bis zu 64 Zeichen.
Proxy-Server und -Port	Geben Sie in diesem Feld die gültige Adresse und den Port des Proxy-Servers ein.

Root-Zertifikat

In dieser Konfiguration können Sie ein Root-Zertifikat für Geräte hochladen. Sie können mehrere **Root-Zertifikat** Konfigurationen hinzufügen. Suchen Sie im **Datei** Feld nach dem relevanten Zertifikat und klicken Sie auf **Übertragen**. Der Name des Zertifikats wird im **Zertifikatsname** Feld angezeigt.

Hinweis: Das hier hochgeladene Zertifikat ist nur für dieses Profil verfügbar. Wenn Sie Zertifikate in anderen Profilen benötigen, müssen Sie diese erneut hochladen.

Client-Zertifikat

In dieser Konfiguration können Sie ein Client-Zertifikat für Geräte hochladen. Sie können mehrere **Client-Zertifikat** Konfigurationen hinzufügen. Suchen Sie im **Datei** Feld nach dem relevanten Zertifikat und klicken Sie auf **Übertragen**. Der Name des Zertifikats wird im **Zertifikatsname** Feld angezeigt. Geben Sie das **Kennwort** für das ausgewählte Zertifikat ein.

Hinweis: Das hier hochgeladene Zertifikat ist nur für dieses Profil verfügbar. Wenn Sie Zertifikate in anderen Profilen benötigen, müssen Sie diese erneut hochladen.

SCEP

In dieser Konfiguration können Sie Einstellungen definieren, die es den Geräten ermöglichen, Zertifikate über Simple Certificate Enrollment Protocol (SCEP) von einer Zertifizierungsstelle (Certificate Authority) zu erhalten. Sie können nur eine **SCEP** Konfiguration in einem Profil hinzufügen.

Hinweis: Diese Konfiguration steht nur dann zur Verfügung, wenn SCEP während der Einrichtung von Sophos Mobile Control konfiguriert wurde. SCEP muss während der Installation von Sophos Mobile Control aktiviert werden, siehe *Sophos Mobile Control Installation Guide* (Englisch). Als Superadministrator können Sie dann die erforderlichen SCEP-Einstellungen in der Web-Konsole konfigurieren, siehe *Sophos Mobile Control Super Administrator Guide* (Englisch). Die definierten Einstellungen werden an iOS-Profile übertragen.

Hinweis: Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

Einstellung/Feld	Beschreibung
URL	Geben Sie in diesem Feld die URL des SCEP-Servers ein.
Name	Geben Sie in diesem Feld einen Namen ein, der von der Zertifizierungsstelle verstanden wird. Der Name kann zum Beispiel zur Unterscheidung zwischen Instanzen verwendet werden.
Betreff	Geben Sie in diesem Feld eine Darstellung eines X.500 Namens in Form eines Datenfelds aus OID und Wert ein. Zum Beispiel: /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar. Dies wird wie folgt übersetzt: [[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]
Typ des alternativen Namens des Inhabers	Wählen Sie in diesem Feld den Typ des alternativen Namens für den SCEP-Server: ■ **Ohne** ■ **RFC 822-Name** (Email-Adresse) ■ **DNS-Name** ■ **Uniform Resource Identifier** Wenn Sie eine andere Option als **Ohne** wählen, werden unter dem Feld **Typ des alternativen Namens des Inhabers** die Felder **Wert des alternativen Namens des Inhabers** und **NT-Benutzeranmeldename** angezeigt. Geben Sie die erforderlichen Namensangaben ein.
Challenge	Geben Sie in diesem Feld ein Pre-Shared Secret ein, anhand dessen der SCEP-Server die Anforderung oder den Benutzer identifizieren kann.
Wiederholungen	Legen Sie in diesem Feld fest, wie oft das Gerät einen Übertragungsversuch wiederholen soll, wenn der Server als Antwort "Anstehend" sendet.
RetryDelay	Legen Sie in diesem Feld die Wartezeit in Sekunden zwischen den Versuchen fest.

Einstellung/Feld	Beschreibung
Schlüsselgröße	Wählen Sie in diesem Feld den Schlüsselgröße: ■ **1024** ■ **2048**
Als digitale Signatur verwenden	Wählen Sie diese Option, um festzulegen, dass die Verwendung des Schlüssels als digitale Signatur zulässig ist.
Für Verschlüsselung verwenden	Wählen Sie diese Option, um festzulegen, dass die Verwendung des Schlüssels für die Verschlüsselung zulässig ist.
Signatur	Geben Sie in diesem Feld eine hexadezimale Zeichenfolge als Signatur ein.

17.1.3 Importieren von mit der Apple iPhone Configuration Utility erstellten iOS-Profilen

Sie können mit der Apple iPhone Configuration Utility erstellte Profile in die Web-Konsole importieren.

Hinweis: Die Apple iPhone Configuration Utility steht hier zur Installation zur Verfügung:

- Für Windows: *http://support.apple.com/kb/DL1466*
- Für Mac OS X: *http://support.apple.com/kb/DL1465*

1. Nachdem Sie ein Profil in der Apple iPhone Configuration Utility erstellt haben, exportieren Sie es (unverschlüsselt und unsigniert) und speichern Sie es auf Ihrem Computer.
2. Klicken Sie in der Web-Konsolen-Menüleiste unter **Konfigurationen** - **Apple iOS** auf **Profile**.

   Die **Profile** Ansicht wird angezeigt.

3. Klicken Sie auf die Schaltfläche **Profil importieren**.

   Die **Profil bearbeiten** Ansicht wird angezeigt.

4. Geben Sie einen **Namen** und eine **Version** für das neue Profil ein.
5. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das das Profil gelten soll.
6. Suchen Sie nach dem Profil, das Sie auf Ihrem Computer gespeichert haben, und klicken Sie auf **Übertragen**.

   Das Profil wird in der **Profil bearbeiten** Ansicht angezeigt.

7. Klicken Sie auf die **Speichern** Schaltfläche.

Das Profil steht für die Übertragung zur Verfügung. Es wird in der **Profile** Ansicht angezeigt.

17.2 Erstellen von Profilen für Android-Geräte

1. Klicken Sie im Web-Konsole-Menü unter **Konfigurationen** - **Android** auf **Profile**.

   Die **Profile** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neues Profil anlegen**.

   Die **Profil bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Version** für das neue Profil ein.
4. Geben Sie im **Kennung** Feld eine eindeutige Kennung für das Profil ein.
5. Geben Sie im Feld **Beschreibung** eine Beschreibung für das Profil ein.
6. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das das Profil gelten soll.
7. Klicken Sie auf die **Hinzufügen** Schaltfläche, um Konfigurationen mit Android-Konfigurationseinstellungen zum Profil hinzuzufügen.

   Die **Verfügbare Konfigurationen** Ansicht wird angezeigt.

8. Wählen Sie die Konfiguration aus, die Sie hinzufügen möchten, und klicken Sie auf **Weiter**.

   Die Einstellungen-Ansicht der Konfiguration wird angezeigt.

9. Definieren Sie die erforderlichen Einstellungen. Für eine detaillierte Liste aller verfügbaren Konfigurationen und Einstellungen siehe *Verfügbare Android-Konfigurationen* (Seite 68).
10. Klicken Sie auf die **Übernehmen** Schaltfläche, um Ihre Änderungen zu speichern.

    Die Konfiguration wird in der **Profil bearbeiten** Ansicht unter **Konfigurationen** angezeigt.

11. Wenn Sie alle erforderlichen Konfigurationen hinzugefügt haben, klicken Sie auf die **Speichern** Schaltfläche.

Das Profil steht für die Übertragung zur Verfügung. Es wird in der **Profile** Ansicht angezeigt.

17.2.1 Verfügbare Android-Konfigurationen

Die folgenden Konfigurationen sind für Android-Profile in der **Verfügbare Konfigurationen** Ansicht verfügbar, wenn Sie ein Profil erstellen oder bearbeiten. Einige Konfigurationen lassen sich in einem Profil nur einmal hinzufügen, andere mehrmals.

Hinweis: Die unterstützten Einstellungen richten sich u. U. nach herstellerspezifischen APIs. Je nach Endbenutzergerät haben einige Einstellungen unter Umständen keine Auswirkungen. Weitere Informationen finden Sie in der Feature Matrix im *Sophos Mobile Control Technical Guide* (Englisch).

Kennwortrichtlinien

In dieser Konfiguration können Sie Kennwortrichtlinien für Geräte definieren. Sie können nur eine **Kennwortrichtlinien** Konfiguration in einem Profil hinzufügen.

Wenn Sie die **Kennwortrichtlinien** Konfiguration auswählen, wird das **Kennworttyp** Feld angezeigt. Wählen Sie in diesem Feld die Art des Kennworts, dass Sie definieren möchten:

- **Beliebig**

  Wenn Sie diese Einstellung wählen, müssen Benutzer ein Kennwort auf dem Endgerät einstellen. Für das Kennwort gelten jedoch keine Anforderungen oder Einschränkungen. Wenn Sie diese Option wählen, sind für die **Kennwortrichtlinien** Konfiguration keine weiteren Einstellungen erforderlich.

- **Alphabetisch**
- **PIN**
- **Alphanumerisch**
- **Komplex**

Wenn Sie **Alphabetisch**, **PIN** oder **Alphanumerisch** auswählen, werden die folgenden Felder angezeigt:

Einstellung/Feld	Beschreibung
Minimale Kennwortlänge	Gibt an, wie viele Zeichen ein Kennwort mindestens enthalten muss.
Inaktivitätszeit in Sekunden bis zur Abfrage des Kennworts	In diesem Feld können Sie festlegen, wann (in Sekunden) das Gerät nach Nichtbenutzung gesperrt werden soll. Das Gerät lässt sich durch Eingabe des Kennworts entsperren.
Gültigkeitsdauer des Kennworts (Tage)	Fordert eine Änderung des Kennworts im angegebenen Intervall (in Tagen).
Maximale Anzahl fehlerhafter Loginversuche	In diesem Feld können Sie die Höchstanzahl an fehlgeschlagenen Eingabeversuchen für das Kennwort eingeben. Nach Erreichen der Höchstanzahl wird das Gerät zurückgesetzt.
Anzahl der letzten Kennwörter, die nicht benutzt werden dürfen	In diesem Feld können Sie festlegen, wie viele alte Kennwörter gespeichert und mit neu definierten Kennwörtern verglichen werden. Wenn ein Benutzer ein neues Kennwort festlegt, wird es nicht akzeptiert, wenn es mit einem bereits benutzten Kennwort übereinstimmt. Wertebereich: 1 bis 5 oder kein Wert.

Wenn Sie **Komplex** auswählen, werden zusätzlich zu den für die anderen Kennworttypen angezeigten Felder die folgenden Felder angezeigt:

Einstellung/Feld	Beschreibung
Minimale Anzahl an Buchstaben	Gibt an, wie viele Buchstaben ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Kleinbuchstaben	Gibt an, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Zeichen, die kein Buchstabe sind	Gibt an, wie viele nicht-alphabetische Zeichen (zum Beispiel & oder !) ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Zahlen	Gibt an, wie viele Zahlen ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Sonderzeichen	Gibt an, wie viele Sonderzeichen (zum Beispiel !"§$%&/()=,.-;:_@<>) ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Großbuchstaben	Gibt an, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.

Einschränkungen

In dieser Konfiguration können Sie Einschränkungen für Geräte definieren. Sie können nur eine **Einschränkungen** Konfiguration in einem Profil hinzufügen.

Einstellung/Feld	Beschreibung
Auf Werkseinstellungen zurücksetzen erlauben	Wenn Sie diese Option deaktivieren, können Benutzer Ihre Geräte nicht auf die Werkseinstellungen zurücksetzen.
Einstellungen ändern erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Einstellungen auf ihren Geräten ändern. Je nach Gerät wird das Symbol für die Einstellungen entfernt.
Backup erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine System-Backups erstellen. Google Backup wird deaktiviert. Andere Backup-Verfahren (zum Beispiel Sophos Mobile Control Backups) bleiben aktiv.
Bluetooth erlauben	Wenn Sie diese Option deaktivieren, wird Bluetooth auf den Geräten deaktiviert.
Kamera erlauben	Wenn Sie diese Option deaktivieren, werden Kameras vollständig auf den Geräten deaktiviert.

Einstellung/Feld	Beschreibung
Zwischenablage erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Inhalte in die Zwischenablage kopieren.
NFC erlauben	Wenn Sie diese Option deaktivieren, wird NFC (Near Field Communication) auf den Geräten deaktiviert.
Screenshot erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Screenshots vom Display erstellen.
SD-Karte erlauben	Wenn Sie diese Option deaktivieren, können in den Geräten keine SD-Karten verwendet werden. SD-Karten werden deaktiviert.
USB-Debuggen erlauben	Wenn Sie diese Option deaktivieren, wird USB-Debuggen auf den Geräten deaktiviert.
USB erlauben	Wenn Sie diese Option deaktivieren, werden der USB-Speichermodus der USB-Media Player auf den Geräten deaktiviert.
WiFi-Tethering erlauben	Wenn Sie diese Option deaktivieren, wird WiFi-Tethering auf den Geräten deaktiviert.
USB-Tethering erlauben	Wenn Sie diese Option deaktivieren, wird USB-Tethering auf den Geräten deaktiviert.
Bluetooth-Tethering erlauben	Wenn Sie diese Option deaktivieren, wird Bluetooth-Tethering auf den Geräten deaktiviert.

Exchange-ActiveSync

In dieser Konfiguration können Sie die Einstellungen für Ihren Microsoft Exchange Server definieren. Sie können mehrere **Exchange-ActiveSync** Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
Name	Geben Sie in diesem Feld einen Konto-Namen an.
Server-Adresse	Geben Sie in diesem Feld die Adresse des Microsoft Exchange Servers an.
Domain	Geben Sie in diesem Feld die Domäne für das Konto an.

Einstellung/Feld	Beschreibung
Benutzer	Geben Sie in diesem Feld den Benutzer für das Konto an.
E-Mail-Adresse	Geben Sie in diesem Feld die E-Mail-Adresse für das Konto an.
Kennwort	Geben Sie in diesem Feld das Kennwort für das Konto an.
Synchronisationszeitraum in Tagen	Wählen Sie in diesem Feld den Zeitraum für die E-Mail-Synchronisierung. Dabei handelt es sich um die Anzahl an Tagen, für die E-Mails synchronisiert werden. Wenn Sie hier einen Zeitraum angeben, werden nicht alle im Posteingang enthaltenen E-Mails auf dem Mobilgerät synchronisiert, sondern nur die E-Mails aus dem angegebenen Zeitraum. Sie können folgende Optionen auswählen: ■ **Ein Tag** ■ **Drei Tage** ■ **Eine Woche** ■ **Zwei Wochen** ■ **Ein Monat**
Synchronisationsintervall	Wählen Sie in diesem Feld den Abstand zwischen den einzelnen E-Mail-Synchronisierungsvorgängen: ■ **Niemals** ■ **5 Minuten** ■ **10 Minuten** ■ **15 Minuten** ■ **30 Minuten** ■ **1 Stunde**
Absender	Geben Sie in diesem Feld einen Absendernamen für das Konto an. Alle mit diesem Konto gesendeten E-Mails benutzen diesen Absendernamen.
SSL	Wählen Sie diese Option, um für die gesamte Kommunikation SSL (Secure Socket Layer) zu verwenden.

Einstellung/Feld	Beschreibung
Standardkonto	Wählen Sie diese Option, um das Konto als das Standard-E-Mail-Konto zu definieren.
Erlaube alle Zertifikate	Wählen Sie diese Option, um für Übertragungsvorgänge durch den E-Mail Server alle Zertifikate zuzulassen.
Client-Zertifikat	Wählen Sie in diesem Feld das Client-Zertifikat für die Verbindung zu ActiveSync.

WiFi

In dieser Konfiguration geben Sie die Einstellungen für die Verbindung mit WiFi-Netzwerken an. Sie können mehrere **WiFi** Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
SSID	Geben Sie in diesem Feld die ID des Drahtlosnetzwerks an.
Sicherheitstyp	In diesem Feld wählen Sie den Sicherheitstyp des WiFi-Netzwerks: ■ **Ohne** ■ **WEP** ■ **WPA** ■ **EAP/PEAP** ■ **EAP/LEAP** ■ **EAP/TLS** ■ **EAP/TTLS** ■ **EAP/FAST** Wenn Sie die persönlichen Einstellungen **WEP** oder **WPA** wählen, wird ein **Kennwort** Feld angezeigt. Geben Sie das relevante Kennwort ein. Wenn Sie die EAP-Einstellungen wählen, werden die Felder **Identität**, **Anonyme Identität** und **Kennwort** angezeigt. Geben Sie die erforderlichen EAP-Informationen ein. Wenn Sie die EAP-Einstellung **EAP TTLS** wählen, wird zusätzlich das Feld **Phase**

Einstellung/Feld	Beschreibung
	2-Autorisierung angezeigt. Wählen Sie die Art der Autorisierung: ■ **PAP** ■ **CHAP** ■ **MSCHAP** ■ **MSCHAPv2**

VPN

In dieser Konfiguration können Sie VPN-Einstellungen für Netzwerke definieren. Sie können mehrere **VPN** Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
Verbindungsname	Geben Sie in diesem Feld den Namen der Verbindung ein, der auf dem Gerät angezeigt wird.
Server	Geben Sie in diesem Feld den Host-Namen oder die IP-Adresse des Servers ein.
Verbindungstyp	Wählen Sie in diesem Feld den Verbindungstyp: ■ **IPsec (PSK)** Wenn Sie diesen Typ auswählen, werden die Felder **Benutzer**, **Kennwort** und **IPsec (PSK)** angezeigt. Geben Sie den Benutzer und das Kennwort ein. Geben Sie im Feld **IPsec (PSK)** den Pre-shared Key für die Authentisierung ein. ■ **IPSec (Zertifikat)** Wenn Sie diesen Typ auswählen, werden die Felder **Client-Zertifikat**, **Root-Zertifikat**, **Benutzer** und **Kennwort** angezeigt. Wählen Sie in den Feldern **Client-Zertifikat** und **Root-Zertifikat** die relevanten Zertifikate. Geben Sie außerdem den **Benutzer** und das zugehörige **Kennwort** ein.

Root-Zertifikat

In dieser Konfiguration können Sie ein Root-Zertifikat für Geräte hochladen. Sie können mehrere **Root-Zertifikat** Konfigurationen hinzufügen. Suchen Sie im **Datei** Feld nach dem relevanten Zertifikat und klicken Sie auf **Übertragen**. Der Name des Zertifikats wird im **Zertifikatsname** Feld angezeigt.

Hinweis: Das hier hochgeladene Zertifikat ist nur für dieses Profil verfügbar. Wenn Sie Zertifikate in anderen Profilen benötigen, müssen Sie diese erneut hochladen.

Client-Zertifikat

In dieser Konfiguration können Sie ein Client-Zertifikat für Geräte hochladen. Sie können mehrere **Client-Zertifikat** Konfigurationen hinzufügen. Suchen Sie im **Datei** Feld nach dem relevanten Zertifikat und klicken Sie auf **Übertragen**. Der Name des Zertifikats wird im **Zertifikatsname** Feld angezeigt. Geben Sie das **Kennwort** für das ausgewählte Zertifikat ein.

Hinweis: Das hier hochgeladene Zertifikat ist nur für dieses Profil verfügbar. Wenn Sie Zertifikate in anderen Profilen benötigen, müssen Sie diese erneut hochladen.

17.3 Hochladen von Vorlagen für Windows Mobile Profile

Für das Erstellen von Windows Mobile Profilen können Sie Vorlagen verwenden. Hierzu müssen Sie die von Sophos gelieferten Vorlagen in der Web-Konsole hochladen.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Konfigurationen** bei **Windows Mobile** auf **Profilvorlagen**.

   Die **Profilevorlagen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neue Vorlage anlegen**

   Die **Profilvorlage bearbeiten** Ansicht wird angezeigt.

3. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das die Vorlage gelten soll.
4. Wählen Sie die von Sophos gelieferte Vorlage aus und klicken Sie auf **Übertragen**.
5. Klicken Sie auf die **Speichern** Schaltfläche.

Die Vorlage steht zum Erstellen von Profilen für Windows Mobile Geräten zur Verfügung. Sie wird in der **Profilvorlagen** Ansicht angezeigt.

17.4 Erstellen von Profilen für Windows-Geräte

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Konfigurationen** bei **Windows Mobile** auf **Profile**.

   Die **Profile** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neues Profil anlegen**.

   Die **Profilvorlage wählen** Ansicht wird angezeigt.

3. Wählen Sie die zu benutzende Vorlage aus und klicken Sie auf **Weiter**.

   Die **Profil bearbeiten** Ansicht wird angezeigt.

4. Geben Sie einen **Namen** und eine **Version** für das neue Profil ein.
5. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das das Profil gelten soll.
6. Klicken Sie in den angezeigten Profileinstellungen auf die einzelnen Einstellungen und geben Sie die erforderlichen Informationen ein. Wählen Sie unter **Send settings** die Option **true** oder **false** und klicken Sie auf **Übernehmen**.

   Hinweis: Klicken Sie für jede Einstellung auf **Übernehmen**. Andernfalls gehen Ihre Einstellungen verloren.

7. Wenn Sie Ihre Änderungen vorgenommen haben, klicken Sie auf die **Speichern** Schaltfläche.

Das Profil steht für die Übertragung zur Verfügung. Es wird in der **Profile** Ansicht angezeigt.

17.5 Platzhalter für Profile

Generische Profile können Platzhalter enthalten, die zum Zeitpunkt der Auftragsausführung durch Benutzerdaten ersetzt werden. Sie können folgende Platzhalter in Profilen verwenden:

ActiveDirectory Platzhalter

- %_EMAILADDRESS_%
- %_USERNAME_%

Geräteeigenschaften-Platzhalter:

%_DEVPROP(Eigenschaftsname)_%

Mit diesem Platzhalter können Sie zum Beispiel die IMEI des Geräts angeben: %_DEVPROP(IMEI)_%

17.6 Übertragung von Profilen

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Konfigurationen** auf **Übertragung** beim gewünschten Mobilgerätetyp: **Apple iOS**, **Android** oder **Windows Mobile**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

2. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Wählen Sie einzelne Geräte aus, an die das Profil übertragen werden soll.
   - Klicken Sie auf die **Gruppenauswahl** Schaltfläche, um die **Gerätegruppe(n) wählen** Ansicht zu öffnen. Wählen Sie dann ein oder mehrere Gerätegruppen für die Übertragung des Profils aus.

3. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Die **Profil wählen** Ansicht wird angezeigt.

4. Wählen Sie das Profil aus, das Sie hinzufügen möchten, und klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

5. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
6. Klicken Sie auf die **Fertigstellen** Schaltfläche.

   Die **Auftragsstatus** Ansicht wird angezeigt.

Das Profil wird zum angegebenen Zeitpunkt auf die ausgewählten Geräte übertragen.

17.7 Herunterladen von iOS- und Android-Profilen aus der Web-Konsole

Sie können die iOS- und Android-Profile, die Sie konfiguriert haben, aus der Web-Konsole herunterladen. Dies ist zum Beispiel nützlich, wenn Sie die definierten Einstellungen an den Sophos Support weitergeben möchten.

1. Gehen Sie im Web-Konsole-Menü zu **Konfigurationen** und klicken Sie unter **Apple iOS** oder **Android** auf **Profile**.
2. Klicken Sie auf das **Anzeigen** Lupensymbol neben dem gewünschten Profil.

   Die **Profil anzeigen** Ansicht wird angezeigt.

3. Klicken Sie auf die **Download** Schaltfläche.

   Ein Dialog für den Download wird angezeigt.

4. Laden Sie das Profil an einen Speicherort Ihrer Wahl herunter.

iOS-Profile werden als .config-Dateien gespeichert, Android-Profile als .xml-Dateien.

18 Mit Auftragspaketen arbeiten

Mit Auftragspaketen können Sie mehrere Aufträge für Mobilgeräte in einer Transaktion bündeln. Somit können Sie alle Aufträge bündeln, die zur vollständigen Registrierung eines Geräts notwendig sind:

- Provisionierung des Geräts
- Anwendung der erforderlichen Richtlinien
- Installation von erforderlichen Applikationen (zum Beispiel Managed Apps für Apple iOS-Geräte)

Sie können auch Wipe-Befehle in Auftragspakete einbeziehen, um Geräte, die nicht mehr den Compliance-Regeln entsprechen (zum Beispiel durch Jailbreak oder Root Access), auf Ihren Fabrikzustand zurückzusetzen. Für weitere Informationen siehe *Konfigurieren von Compliance-Einstellungen* (Seite 27).

18.1 Erstellen von Auftragspaketen

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Auftragspakete** auf **Pakete**.

   Die **Auftragspakete** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neues Auftragspaket anlegen**.

   Die **Auftragspaket bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Version** für das neue Auftragspaket ein.
4. Wählen Sie unter **Betriebssysteme** die Betriebssysteme, für die das neue Auftragspaket gelten soll.
5. Klicken Sie unter **Aufträge** auf die **Neuen Auftrag anlegen** Schaltfläche.

   Der Dialog **Typ wählen** wird angezeigt.

6. Wählen Sie den Auftragstyp und klicken Sie auf **Weiter**.

   Die nächste Ansicht hängt vom gewählten Auftragstyp ab. Wenn Sie zum Beispiel den Typ **Installation eines Softwarepaketes** ausgewählt haben, wird die **Paket wählen** Ansicht angezeigt.

7. Folgen Sie den Schritten des Assistenten, um den gewünschten Auftrag hinzuzufügen.
8. Wiederholen Sie diesen Vorgang, um weitere Aufträge hinzuzufügen. Beim Hinzufügen neuer Aufträge können Sie Ihre eigenen aussagekräftigen Namen angeben. Diese Auftragsnamen werden während der Installation im Self Service Portal angezeigt. Mit den Sortier-Pfeilsymbolen auf der rechten Seite der **Aufträge** Liste können Sie die Installationsreihenfolge für die ausgewählte Aufträge festlegen.
9. Wenn Sie alle erforderlichen Aufträge zum Auftragspaket hinzugefügt haben, klicken Sie auf die **Speichern** Schaltfläche in der **Auftragspaket bearbeiten** Ansicht.

Das Auftragspaket steht für die Übertragung zur Verfügung. Es wird in der **Auftragspakete** Ansicht angezeigt.

18.2 Duplizieren von Auftragspaketen

Da das Erstellen eines Auftragspakets zeitaufwändig sein kann, können Sie bereits vorhandene Auftragspakete duplizieren. Diese Funktion ist hilfreich, wenn mehrere umfangreiche Auftragspakete mit ähnlichen Aufträgen erforderlich sind. Es müssen dann nur wenige Aufträge gelöscht oder hinzugefügt werden.

Hinweis: Sie können Auftragspakete nur dann duplizieren, wenn sie nicht gleichzeitig bearbeitet werden. Die Kopien werden mit "Copy of" und dem Namen des Originalprofils benannt. Sie können die Namen der Pakete nach Ihren Anforderungen ändern.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Auftragspakete** auf **Pakete**.

   Die **Auftragspakete** Ansicht wird angezeigt.

2. Klicken Sie bei dem Auftragspaket, das Sie duplizieren möchten, auf das **Anzeigen** Lupensymbol.

   Die **Auftragspaket anzeigen** Ansicht wird angezeigt.

3. Klicken Sie auf die **Dieses Paket duplizieren** Schaltfläche.

Das Auftragspaket wird dupliziert und in der **Auftragspakete** Ansicht angezeigt. Sie können das duplizierte Auftragspaket nun bearbeiten. Um das Auftragspaket zu bearbeiten, klicken Sie auf das **Bearbeiten** Bleistiftsymbol neben dem Paket.

18.3 Übertragen von Auftragspaketen

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Auftragspakete** auf **Übertragung**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

2. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Wählen Sie einzelne Geräte aus, an die das Auftragspaket übertragen werden soll.
   - Klicken Sie auf die **Gruppenauswahl** Schaltfläche, um die **Gerätegruppe(n) wählen** Ansicht zu öffnen. Wählen Sie dann ein oder mehrere Gerätegruppen für die Übertragung des Auftragspakets aus.

3. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Die **Auftragspaket wählen** Ansicht wird angezeigt.

4. Wählen Sie das Auftragspaket, das übertragen werden soll, und klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

5. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.

6. Klicken Sie auf die **Fertigstellen** Schaltfläche.

   Die **Auftragsstatus** Ansicht wird angezeigt.

Das Auftragspaket wird zum angegebenen Zeitpunkt auf die ausgewählten Geräte übertragen.

19 Mit Kommandopaketen arbeiten

Hinweis: Kommandopakete sind nur für Android und Windows Mobile Geräte verfügbar.

Mit Kommandopaketen können Sie verschiedene Kommandos für die Konfiguration von mehreren Funktionen in einer Übertragung bündeln. Dies ist besonders hilfreich, wenn eine Reihe von Geräten identisch konfiguriert werden soll.

Hinweis: Falsch verwendete Kommandos können eine Sperre oder sogar eine Beschädigung von Geräten auslösen. Diese Funktion sollten daher nur erfahrene Benutzer verwenden. Wir empfehlen dringend, die Kommandos vor der Verteilung bei einem einzelnen Gerät zu testen.

19.1 Erstellen von Kommandopaketen

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Kommandopakete** auf **Pakete**.

   Die **Kommandopakete** Ansicht wird angezeigt.

2. Klicken Sie auf die **Neues Paket anlegen** Schaltfläche.

   Die **Kommandopaket bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Version** für das neue Kommandopaket ein. Diese beiden Felder sind Pflichtfelder.
4. Wählen Sie unter **Betriebssysteme** die kompatiblen Betriebssysteme für das neue Kommandopaket.
5. Klicken Sie unter **Kommandos** auf die **Neues Kommando hinzufügen** Schaltfläche.

   Die **Kommando wählen** Ansicht wird angezeigt.

   Hinweis: Standardkommandos werden auf allen verfügbaren Plattformen unterstützt. Andere Kommandos werden nur bei spezifischen Plattformen unterstützt. Die Spalten **AND** (Android) und **WIN** (Windows Mobile) neben den Kommandos geben an, für welche Plattform(en) die Kommandos verfügbar sind. Wird nach Auswahl verschiedener Plattformen ein plattformspezifisches Kommando hinzugefügt, so verweigern Geräte, die die spezifische Funktion nicht unterstützen, das Kommando.

6. Wählen Sie das Kommando aus, das Sie hinzufügen möchten, und klicken Sie auf **Weiter**.

   Die **Kommando bearbeiten** Ansicht wird angezeigt.

7. Geben Sie die erforderlichen Parameter für das Kommando ein und klicken Sie auf die **Übernehmen** Schaltfläche.

   Die **Kommandopaket bearbeiten** Ansicht wird angezeigt. Das neue Kommando wird unter **Kommandos** angezeigt.

8. Fügen Sie nach Wunsch weitere Kommandos hinzu. Mit den Sortier-Pfeilsymbolen auf der rechten Seite der **Kommandos** Liste können Sie die Installationsreihenfolge für die ausgewählten Kommandos festlegen.
9. Wenn Sie alle erforderlichen Kommandos hinzugefügt haben, klicken Sie auf die **Speichern** Schaltfläche.

Das Kommandopaket steht für die Übertragung zur Verfügung. Es wird in der **Kommandopakete** Ansicht angezeigt.

19.1.1 Parameter für den Befehl setConfiguration

Mit dem Befehl setConfiguration stellen Sie Werte in der Konfiguration des Sophos Mobile Client ein. Der Befehl bietet folgende Parameter:

Parameter	Beschreibung	Wertetyp	Werte-bereich	Standard	WM	AND
AdminSMS	Die Administrator SMS Telefonnummer für IMSI-Änderungen.	Zeichen-folge			✓	✓
ImsiChange NotifyDelay	Verzögerung für die Überprüfung auf IMSI-Änderungen in Sekunden (-1 = aus, >= 0: an).	Zahl	-1 - 1800	-1	✓	✓
MaxSyncGap	Intervall für die automatische Synchronisierung in Minuten (0: aus).	Zahl	0 - 2147483647	0	✓	✓

19.2 Duplizieren von Kommandopaketen

Da das Erstellen eines Kommandopakets zeitaufwändig sein kann, können Sie bereits vorhandene Kommandopakete duplizieren. Diese Funktion ist hilfreich, wenn mehrere umfangreiche Kommandopakete mit ähnlichen Kommandos erforderlich sind. Es müssen dann nur wenige Befehle gelöscht oder hinzugefügt werden.

Hinweis: Sie können Kommandopakete nur dann duplizieren, wenn sie nicht gleichzeitig bearbeitet werden. Die Kopien werden mit "Copy of" und dem Namen des Originalprofils benannt. Sie können die Namen der Pakete nach Ihren Anforderungen ändern.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Kommandopakete** auf **Pakete**.

   Die **Kommandopakete** Ansicht wird angezeigt.

2. Klicken Sie bei dem Kommandopaket, das Sie duplizieren möchten, auf das **Anzeigen** Lupensymbol.

   Die **Kommandopaket anzeigen** Ansicht wird angezeigt.

3. Klicken Sie auf die **Dieses Paket duplizieren** Schaltfläche.

Das Kommandopaket wird dupliziert und in der **Kommandopakete** Ansicht angezeigt. Sie können das duplizierte Kommandopaket nun bearbeiten. Um das Kommandopaket zu bearbeiten, klicken Sie auf das **Bearbeiten** Bleistiftsymbol neben dem Paket.

19.3 Übertragen von Kommandopaketen

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Kommandopakete** auf **Übertragung**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

2. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Wählen Sie einzelne Geräte aus, an die das Kommandopaket übertragen werden soll.
   - Klicken Sie auf die **Gruppenauswahl** Schaltfläche, um die **Gerätegruppe(n) wählen** Ansicht zu öffnen. Wählen Sie dann ein oder mehrere Gerätegruppen für die Übertragung des Kommandopakets aus.

3. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Die **Kommandopaket wählen** Ansicht wird angezeigt.

4. Wählen Sie das Kommandopaket, das übertragen werden soll, und klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

5. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
6. Klicken Sie auf die **Fertigstellen** Schaltfläche.

   Die **Auftragsstatus** Ansicht wird angezeigt.

Das Kommandopaket wird zum angegebenen Zeitpunkt auf die ausgewählten Geräte übertragen.

20 Konfigurieren der Benutzung des Self Service Portal für Endbenutzer

Mit dem Self Service Portal können Sie IT-Aufwände reduzieren, indem Sie die Endbenutzer dazu berechtigen, ihre eigenen Geräte zu registrieren und andere Aufgaben auszuführen. Hierzu ist keine Unterstützung durch den Helpdesk erforderlich. Die Benutzung des Self Service Portal wird für folgende Plattformen unterstützt:

- Android
- Apple iOS
- Windows Mobile

Für weitere Informationen zur Benutzung des Self Service Portal, siehe die *Sophos Mobile Control Benutzerhandbücher für Android, Apple iOS und Windows Mobile*.

In der Web-Konsole können Sie Einstellungen für die Benutzung des Self Service Portal konfigurieren, zum Beispiel für welche Plattformen die Registrierung über das Self Service Portal aktiv sein soll, oder welche Funktionen im Self Service Portal zur Verfügung stehen sollen. Sie können außerdem die Benutzer des Self Service Portal verwalten.

20.1 Erstellen von Self Service Portal Gruppen mit der internen Benutzerverwaltung

Self Service Portal Konfigurationen werden auf Gruppen von Self Service Portal Benutzern angewendet. Mit der internen Benutzerverwaltung können Sie Self Service Portal Gruppen erstellen und ihnen Benutzer zuweisen. Für weitere Informationen zur Benutzerverwaltung siehe *Verwalten von Self Service Portal Benutzern* (Seite 88).

Hinweis: Die interne Benutzerverwaltung steht nur dann für einen Kunden zur Verfügung, wenn Sie vom Superadministrator aktiviert wurde. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service gilt. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt. In diesem Fall sind Kunden vordefiniert und die interne Benutzerverwaltung wird verwendet.

So erstellen Sie eine Self Service Portal Gruppe:

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Interne Benutzerverwaltung**.

   Die **Benutzer anzeigen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Gruppen anzeigen**.

   Die **Gruppen anzeigen** Ansicht wird angezeigt.

3. Klicken Sie auf die Schaltfläche **Neue Benutzergruppe anlegen**.

   Die **Gruppe bearbeiten** Ansicht wird angezeigt.

4. Geben Sie im Feld **Name** einen Namen für die neue Self Service Portal Gruppe ein.

5. Klicken Sie auf die **Speichern** Schaltfläche.

Die neue Self Service Portal Benutzergruppe wird in der **Gruppe anzeigen** Ansicht angezeigt. Wenn Sie neue Benutzer erstellen, können Sie diese der Gruppe zuweisen. Wenn Sie Self Service Portal Einstellungen definieren, können Sie die Gruppe auswählen und Ihr die Einstellungen zuweisen.

20.2 Konfigurieren von Self Service Portal Einstellungen

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Einstellungen**.

   Die **Einstellungen** Ansicht wird angezeigt.

2. Wechseln Sie in die **Self Service Portal** Registerkarte.
3. Zuerst konfigurieren Sie die Gruppeneinstellungen, zum Beispiel die Gerätegruppen, zu denen über das Self Service Portal registrierte Geräte hinzugefügt werden, und das Auftragspaket, das auf Geräten ausgeführt wird.

   Wenn Sie LDAP-Benutzerverwaltung verwenden, können Sie Geräte basierend auf der Gruppenzugehörigkeit zu Gruppen und Profilen zuweisen.

   Hinweis: Die LDAP-Benutzerverwaltung muss für den relevanten Kunden in der Kundenveraltung konfiguriert werden. Informationen zur Konfiguration der LDAP-Benutzerverwaltung für einen Kunden finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service gilt. In diesem Fall sind Kunden vordefiniert und die interne Benutzerverwaltung wird verwendet. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

   a) Klicken Sie unter **Gruppeneinstellungen** auf die **Hinzufügen** Schaltfläche.

      Die **SSP Konfiguration bearbeiten** Ansicht wird angezeigt.

   b) Geben Sie einen **Namen** für die Self Service Portal Konfigurationsgruppe ein.

   c) Geben Sie im Feld **LDAP Gruppe** die Self Service Portal Gruppe ein, die Sie in der internen Benutzerverwaltung definiert haben, oder die Active Directory Gruppe mit ihrem vollen LDAP-Pfad oder Platzhaltern. In diesem Feld können Sie mit einem Asterisk (*) als erstes, letztes oder einziges Zeichen mehrere Gruppen angeben. Zum Beispiel: Geben Sie Dev* ein, um alle Gruppennamen, die mit "Dev" beginnen, anzugeben. Geben Sie * ein, um alle verfügbaren Gruppen anzugeben.

   d) Wählen Sie unter **Plattform** die Plattformen, die im Self Service Portal zur Verfügung stehen sollen.

   e) Wählen Sie unter **Einfügen in Geräteruppe** die Gruppe, zu der das Gerät hinzugefügt werden soll.

      Hinweis: In der Web-Konsole steht eine **Default** Gerätegruppe zur Verfügung. Wenn Sie noch keine eigenen Gerätegruppen definiert haben, können Sie Geräte zu dieser Gruppe hinzufügen. Für weitere Informationen siehe *Erstellen von Gerätegruppen* (Seite 36).

   f) Wählen Sie unter **Auftragspaket**, die auszuführenden Auftragspakete.

Hinweis: Sie müssen die Auftragspakete zuerst in der Web-Konsole anlegen. Wenn Sie noch kein Auftragspaket erstellt haben, aktualisieren Sie die Self Service Portal Einstellungen danach. Für Informationen zur Erstellung eines Auftragspakets siehe *Mit Auftragspaketen arbeiten* (Seite 78). Für weitere Informationen zu den Anforderungen für ein Auftragspaket, das für die Ersteinrichtung über das Self Service Portal verwendet werden soll, siehe die *Sophos Mobile Control Startup-Anleitung* oder die *Sophos Mobile Control as a Service Startup-Anleitung*.

g) Klicken Sie auf die **Übernehmen** Schaltfläche.

4. Unter **Vereinbarungstext** können Sie eine Mobil-Richtlinie, einen Disclaimer oder eine Vereinbarung konfigurieren. Dieser Text wird im ersten Schritt angezeigt, wenn Endbenutzer Geräte registrieren. Die Benutzer müssen bestätigen, dass sie diesen Text gelesen haben, um fortfahren zu können.

   Für den Text werden einfache HTML-Formatierungs-Tags unterstützt. Der Text wird entsprechend im jeweiligen Browser angezeigt.

5. Unter **Post Install Text** können Sie einen Text konfigurieren, der im Self Service Portal nach den automatischen Installationsschritten angezeigt wird, um dem Benutzer Hilfestellung bei den darauf folgenden erforderlichen Schritten (z. B. Konfiguration des Servers in der iOS App oder Konfiguration des Android Mail Client) zu bieten.

   Für den Text werden einfache HTML-Formatierungs-Tags unterstützt. Der Text wird entsprechend im jeweiligen Browser angezeigt.

6. Wählen Sie im **Maximale Anzahl an Geräten** Feld die maximale Anzahl an Geräten, die ein Benutzer über das Self Service Portal registrieren kann. Durch Festlegung einer maximalen Anzahl können Sie Lizenzüberschreitungen vermeiden.
7. Wählen Sie unter **Verfügbare SSP Funktionen** die Funktionen, die Benutzern im Self Service Portal zur Verfügung stehen sollen. So ist es unter Umständen sinnvoll, die Zurücksetzen-Funktion zu deaktivieren, da ein verlorenes Gerät eine erhebliches Compliance-Risiko darstellt und hier unter Umständen zusätzliche Aktionen mit Unterstützung durch den Helpdesk erforderlich sind. Die Funktionen variieren je nach Mobilgerätetyp (Plattform). Im *Sophos Mobile Control Technical Guide* (Englisch) finden Sie eine Matrix der für die verschiedenen Gerätetypen unterstützten Features. Sie können folgende Funktionen auswählen:

   - **Gerät lokalisieren**

     Mit dieser Funktion können Benutzer Ihre Android- oder iOS-Geräte bei Verlust oder Diebstahl orten.

   - **Gerät sperren**

     Mit dieser Funktion können Benutzer Ihre Geräte bei Verlust oder Diebstahl sperren.

   - **Neukonfiguration**

     Mit dieser Funktion können Benutzer Ihre Geräte neu konfigurieren, wenn Sophos Mobile Control vom Gerät entfernt wurde, das Gerät jedoch noch registriert ist.

   - **Richtlinienverletzungen anzeigen**

     Mit dieser Funktion können Benutzer die Compliance-Verletzungen für die für sie registrierten Geräte im Self Service Portal einsehen.

- **Daten aktualisieren**

  Mit dieser Funktion können Benutzer Ihre Geräte manuell mit dem Sophos Mobile Control Server synchronisieren. Dies ist zum Beispiel nützlich, wenn das Gerät längere Zeit ausgeschaltet war und daher nicht mit dem Server synchronisiert wurde. In diesem Fall ist das Gerät unter Umständen nicht compliant (je nach konfigurierten Compliance-Einstellungen) und muss mit dem Server synchronisiert werden, damit es die Richtlinien wieder erfüllt.

- **Gerät zurücksetzen**

  Mit dieser Funktion können Benutzer Ihre registrierten Geräte bei Verlust oder Diebstahl auf den Werkszustand zurücksetzen. Alle Daten auf dem Gerät werden gelöscht.

- **Gerät deregistrieren**

  Mit dieser Funktion können Benutzer Geräte deregistrieren, die nicht mehr benutzt werden. Dies ist zum Beispiel nützlich, wenn die Anzahl an Geräten, die Benutzer über das Self Service Portal registrieren können, begrenzt ist.

- **Nicht registriertes Gerät löschen**

  Mit dieser Funktion können Benutzer deregistrierte Geräte löschen. Die ist zum Beispiel für das Freigeben benutzter Lizenzen nützlich.

- **Sophos Mobile Control-App aktivieren**

  Mit dieser Funktion können Benutzer von Apple iOS Geräten die Sophos Mobile Control App nach der Installation auf Ihren Geräten aktivieren.

  Hinweis: Dies ist ein notwendiger Schritte für das Einrichten von Sophos Mobile Control auf Apple iOS Geräten. Um sicherzustellen, dass die Aktivierung funktioniert, muss die App zuvor einmal auf dem Gerät geöffnet werden. Wenn Sie die Registrierung und Ersteinrichtung von Apple iOS Geräten über das Self Service Portal für Benutzer ermöglichen möchten, wählen Sie diese Funktion aus.

8. Wenn Sie alle erforderlichen Einstellungen in der **Self Service Portal** Registerkarte konfiguriert haben, klicken Sie auf die **Speichern** Schaltfläche.
9. Wechseln Sie in die **SSP Welcome E-Mail** Registerkarte. In dieser Registerkarte konfigurieren Sie die Willkommens-E-Mail, die an Self Service Portal Benutzer gesendet wird, um diese über ihre Anmeldedaten zu informieren.

   Hinweis: Diese Mail wird nur für Self Service Portal Benutzer gesendet, die über die interne Benutzerverwaltung verwaltet werden, siehe *Verwalten von Self Service Portal Benutzern* (Seite 88).

10. Geben Sie im **Absender** Feld die E-Mail-Absenderadresse ein. Geben Sie im **Betreff** Feld einen E-Mail-Betreff ein, zum Beispiel "Willkommen beim Sophos Mobile Control Self Service Portal".
11. Definieren Sie im Textfeld den Inhalt der E-Mail. Die folgenden Platzhalter sind verfügbar und werden in den E-Mails durch die entsprechenden Werte ersetzt.

    - _RESET_TOKEN_LINK_
    - _LOGINNAME_
    - _FIRSTNAME_

- _LASTNAME_

  Benutzen Sie den Platzhalter _RESET_TOKEN_LINK_, um einen Link für das Erzeugen eines Kennworts für den Benutzer hinzuzufügen. Dieser Link ist für die Bereitstellung eines Kennworts für den Benutzer erforderlich.

12. Wenn Sie die Willkommens-E-Mail konfiguriert haben, klicken Sie auf die **Speichern** Schaltfläche.

Hinweis: Als Superadministrator können Sie auch einen Standard-Kunden festlegen, an dem sich die Endbenutzer im Self Service Portal anmelden. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service unterstützt wird. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

20.3 Verwalten von Self Service Portal Benutzern

Sophos Mobile Control bietet verschiedene Verfahren für die Verwaltung von Self Service Portal Benutzern.

Hinweis: Das verwendete Verfahren ist kundenspezifisch und wird beim Erstellen des Kunden festgelegt. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service gilt. In diesem Fall sind die Kunden vordefiniert. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

- Interne Benutzerverwaltung

  Mit der interenen Benutzerverwaltung können Sie Benutzer durch manuelles Hinzufügen in der Web-Konsole oder durch Importieren aus einer .csv-Datei erstellen.

- LDAP-Benutzerverwaltung

  Mit der LDAP-Benutzerverwaltung können Sie Geräte zu Gruppen und Profilen auf der Grundlage der Active Directory/LDAP Zugehörigkeit zuweisen. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

20.3.1 Erstellen von Self Service Portal Benutzern mit der internen Benutzerverwaltung

Voraussetzung: Die interne Benutzerverwaltung ist für den Kunden, an dem Sie angemeldet sind, aktiviert. Für lokale Installationen erfolgt dies durch den Superadministrator in der Kundenverwaltung. Für weitere Informationen siehe den *Sophos Mobile Control Super Administrator Guide* (Englisch). Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service gilt. In diesem Fall sind die Kunden vordefiniert. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Interne Benutzerverwaltung**.

   Die **Benutzer anzeigen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neuen Benutzer anlegen**.

   Die **Benutzer bearbeiten** Ansicht wird angezeigt.

3. Definieren Sie in der **Benutzer bearbeiten** Ansicht die folgenden Einstellungen:

   a) Stellen Sie sicher, dass das Feld **Welcome Mail versenden** ausgewählt ist. Dieses Feld wird angezeigt, wenn Sie unter **Einstellungen** in der Registerkarte **SSP Welcome-E-Mail** eine Willkommens-E-Mail konfiguriert haben, siehe *Konfigurieren von Self Service Portal Einstellungen* (Seite 85). Wenn dieses Feld nicht angezeigt wird, konfigurieren Sie zuerst eine Willkommens-E-Mail. Diese Mail muss alle erforderlichen Anmeldedaten enthalten.

   b) **Benutzername**

   c) **Nachname**

   d) **Vorname**

   e) **E-Mail**

   f) **Telefonnummer** (optional)

   g) **Gruppen**

4. Klicken Sie auf die **Speichern** Schaltfläche.

Der neue Self Service Portal Benutzer wird in der **Benutzer anzeigen** Ansicht angezeigt. Eine E-Mail mit der Self Service Portal URL und den Anmeldedaten wird an den Benutzer geschickt.

Von der **Benutzer anzeigen** Ansicht aus können Sie die Benutzerdetails einsehen, bearbeiten und Benutzer löschen.

20.3.2 Importieren von Benutzern mit der internen Benutzerverwaltung

Mit der internen Benutzerverwaltung können Sie neue Self Service Portal Benutzer hinzufügen, indem Sie eine .csv-Datei mit bis zu 300 Benutzern importieren.

Auf der Import-Seite steht eine Musterdatei mit den korrekten Spaltennamen und der richtigen Spaltenreihenfolge zum Download zur Verfügung.

Hinweis: Verwenden Sie einen Text-Editor zum Bearbeiten der .csv-Datei. Wenn Sie Microsoft Excel verwenden, werden die eingegebenen Werte u. U. nicht korrekt aufgelöst. Speichern Sie die Datei mit der Dateinamenerweiterung .csv.

Voraussetzung: Die interne Benutzerverwaltung ist für den Kunden, an dem Sie angemeldet sind, aktiviert. Weitere Informationen finden Sie im *Sophos Mobile Control Superadministrator Guide* (Englisch). Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service gilt. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt. In diesem Fall sind Kunden vordefiniert und die interne Benutzerverwaltung wird verwendet.

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Interne Benutzerverwaltung**.

   Die **Benutzer anzeigen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Benutzer importieren**.

   Die **Benutzer importieren** Ansicht wird angezeigt.

   Wenn Sie noch keine .csv-Datei mit Benutzern haben, können Sie nun eine Musterdatei herunterladen und diese zum Erstellen Ihrer Importdatei verwenden.

3. Stellen Sie sicher, dass das Feld **Welcome Mails versenden** ausgewählt ist. Dieses Feld wird angezeigt, wenn Sie unter **Einstellungen** in der Registerkarte **SSP Welcome-E-Mail** eine Willkommens-E-Mail konfiguriert haben, siehe *Konfigurieren der Benutzung des Self Service Portal für Endbenutzer* (Seite 84). Wenn dieses Feld nicht angezeigt wird, konfigurieren Sie zuerst eine Willkommens-E-Mail. Diese Mail muss alle erforderlichen Anmeldedaten enthalten.
4. Wählen Sie die zu importierende .csv-Datei aus und klicken Sie auf **Datei hochladen**.

   Die Einträge in der .csv-Datei werden auf Fehler überprüft und auf der Import-Seite angezeigt.

   Hinweis: Wenn die .csv-Datei Fehler enthält, kann sie nicht importiert werden. Neben den relevanten Einträgen wird jeweils eine Fehlermeldung angezeigt. Bearbeiten Sie die .csv-Datei entsprechend und versuchen Sie es noch einmal.

5. Wenn alle Einträge korrekt sind, klicken Sie auf die **Fertigstellen** Schaltfläche.

Die Benutzer werden importiert und in der **Benutzer anzeigen** Ansicht angezeigt.

Von der **Benutzer anzeigen** Ansicht aus können Sie die Benutzerdetails einsehen, bearbeiten und Benutzer löschen.

21 Verwalten von Geräten im Inventar

Das **Inventar** ist das zentrale Modul für die Verwaltung von Geräten. Mit dem **Inventar** haben Sie stets einen aktuellen Überblick zu den registrierten Geräten und den Gerätegruppen. Außerdem können Sie eine Reihe von administrativen Aufgaben durchführen. Nachdem Sie Geräte zu Sophos Mobile Control hinzugefügt haben, können Sie zum Beispiel:

- Gerätedetails einsehen und bearbeiten
- E-Mail-Zugriff für Geräte erlauben oder untersagen

  Hinweis: Diese Funktion ist für Sophos Mobile Control as a Service nicht verfügbar.

- Geräte remote sperren oder entsperren.
- Passcodes/Passwörter von Geräten zurücksetzen
- Geräte bei Verlust oder Diebstahl remote auf den Werkszustand zurücksetzen
- Geräte deregistrieren (Android und iOS)
- Geräte löschen

Für eine Übersicht zu allen verfügbaren Funktionen mit den entsprechenden Funktionsschaltflächen siehe *Ausführen von administrativen Aufgaben* (Seite 98).

21.1 Einsehen von Geräten

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Geräte**.

   Die **Geräte** Ansicht mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, wird angezeigt.

2. Klicken Sie beim gewünschten Gerät auf das Lupensymbol.

Die **Gerät anzeigen** Ansicht für das ausgewählte Gerät wird angezeigt.

21.1.1 Die Gerät anzeigen Ansicht

In der **Gerät anzeigen** Ansicht werden alle relevanten Informationen für ein einzelnes Gerät angezeigt. Oben in der Ansicht werden folgende Informationen angezeigt: **Name**, **Beschreibung**, **Gerätegruppe**, **Telefonnummer**, **Eigentümer** (**Firmengerät** oder **Privates Gerät**) **E-Mail-Adresse**, (für Android- und iOS-Geräte), **Betriebssystem**, **Geräte-ID** und **Letzte Synchronisation**. Für iOS-Geräte wird die **Letzte iOS-App Synchronisation** angezeigt.

Außerdem zeigt die **Gerät anzeigen** Ansicht detaillierte Geräteinformationen in den folgenden Registerkarten. Die angezeigten Registerkarten und Informationen richten sich nach dem Mobilgerätetyp (Plattform).

- **Geräteeigenschaften**

  Zeigt die Geräteeigenschaften, zum Beispiel Eigenschaften für Modell, Modellname, Betriebssystemversion. Bei Android-Geräten werden Smartphones im Root-Zustand

ermittelt und die relevante Eigenschaft wird angezeigt. Bei iOS-Geräten werden Smartphones im Jailbroken-Zustand ermittelt. Die relevante Eigenschaft wird in der Ansicht angezeigt.

- **Eigene Eigenschaften**

  Zeigt die eigenen Eigenschaften. Dies sind Eigenschaften, die Sie selbst anlegen können. Eigene Eigenschaften können zum Beispiel in Platzhaltern verwendet werden, wenn kein Active Directory zur Verfügung steht. Wenn Sie ein Gerät bearbeiten, können Sie hier auch benutzerspezifische Informationen hinzufügen.

- **Interne Eigenschaften**

  Zeigt interne Geräteeigenschaften, z. B. zugelassener Active Sync Traffic, IMEI.

- **Richtlinienverletzungen**

  Diese Registerkarte wird nur für Geräte angezeigt, die nicht compliant sind. Sie zeigt die Richtlinienverletzungen des Geräts. Klicken Sie auf das **Anzeigen** Lupen-Symbol neben einer Richtlinienverletzung um die **Historie** der Richtlinenverletzung einzusehen.

  Sie können die für das Gerät angezeigten Compliance-Informationen von der **Richtlinienverletzungen** Registerkarte aus aktualisieren. Klicken Sie auf das **Bearbeiten** Symbol in der **Richtlinienverletzungen** Registerkarte oder auf das **Neue Aktion hinzufügen** Symbol in der **Historie** Ansicht, um den **Aktion hinzufügen** Dialog anzuzeigen. In diesem Dialog können Sie Informationen zur Aktion eingeben, die aufgrund einer Compliance-Verletzung durchgeführt wurde. Zum Beispiel: Benutzer per E-Mail benachrichtigt.

- **Installierte Software**

  Zeigt die auf dem Gerät installierte Software.

  Für iOS-Geräte zeigt die **Managed** Spalte in der **Installierte Software** Registerkarte die Managed Apps. Die Managed Apps iOS Funktionalität wurde mit iOS 5.0 eingeführt. Mit Sophos Mobile Control können Sie solche Apps auf IOS-Geräte pushen und sie auch unbemerkt wieder entfernen.

  Hinweis: Sophos Mobile Control unterstützt die Managed Apps Funktionalität ab iOS 5.1.

  Für Android-Geräte unterscheidet Sophos Mobile Control zwischen System Apps und Apps, die der Benutzer auf dem Gerät installiert hat.

  Für Android-Geräte wird das Datenvolumen, das von den einzelnen Apps benutzt wird, angezeigt.

  Für iOS-Geräte wird der Speicherplatz angezeigt, den eine App nach der Installation benötigt. Außerdem wird der u. U. zusätzlich benötigte Speicherplat angezeigt. Dieser Speicherplatz ist u. U. für Downloads, Konfigurationen, Einstellungen usw. erforderlich.

  In dieser Registerkarte steht oben links in der Ecke die Schaltfläche **Software installieren** zur Verfügung. Mit dieser Schaltfläche können Sie Software auf dem Gerät installieren. Sie können auch Managed Apps von iOS-Geräten entfernen, indem Sie auf das **Löschen** Symbol neben der relevanten App klicken.

- **Installierte Profile (iOS und Android)**

Zeigt die auf Geräten installierten Profile.

Hinweis: Für Android-Geräte werden die Profile ab der Sophos Mobile Control Client-Version 3.0 angezeigt.

In dieser Registerkarte steht die Schaltfläche **Profil installieren** zur Verfügung. Mit dieser Schaltfläche können Sie Profile auf dem Gerät installieren. Sie können auch Profile vom Gerät entfernen, indem Sie auf das **Löschen** Symbol neben dem relevanten Profil klicken.

In dieser Registerkarte werden auch Provisionierungsprofile aufgelistet.

- **System Software (Android)**

  Zeigt die Android System Software auf dem Gerät an.

  Hinweis: System Software kann nicht vom Gerät entfernt werden.

- **Zertifikate (iOS)**

  Zeigt die auf dem iOS-Gerät benutzten Zertifikate an.

- **Scan-Ergebnisse (SMSec)**

  Diese Registerkarte ist nur dann verfügbar, wenn für den Kunden, an dem Sie angemeldet sind, die Sophos Mobile Security Funktionalität zur Verfügung steht. Die Registerkarte zeigt die Ergebnisse des letzten Sophos Mobile Security Scan-Vorgangs auf dem Gerät. Sophos Mobile Security ist eine Security App für Android-Mobiltelefone und Tablets, die Geräte vor schädlichen Apps schützt und Endbenutzer beim Erkennen von App-Berechtigungen unterstützt, die u. U. ein Sicherheitsrisiko darstellen. Die App kann von der Sophos Mobile Control Web-Konsole verwaltet werden. Für weitere Informationen siehe *Verwaltung von Sophos Mobile Security über Sophos Mobile Control* (Seite 114).

Von der **Gerät anzeigen** Ansicht können Sie direkt in die **Gerät bearbeiten** Ansicht wechseln. Um das derzeit angezeigte Gerät zu bearbeiten, klicken Sie auf die **Bearbeiten** Schaltfläche.

21.2 Einsatz von Filtern im Inventar

Mit Filtern lässt sich die Anzahl an in Listen angezeigten Einträgen nach definierten Kriterien einschränken. Um einen Filter anzuwenden, klicken Sie auf die **Filter** Schaltfläche im Header der Web-Konsole. Der Filter wird geöffnet und Sie können die gewünschten Filterkriterien definieren.

Im **Inventar** können Sie folgende Filter verwenden:

- Gerätefilter
- Gerätegruppenfilter

21.2.1 Anwenden des Gerätefilters

Mit dem Gerätefilter lassen sich Gerätelisten filtern.

Hinweis: Die Filter gelten nicht nur für die derzeit angezeigte Funktion, sondern für alle Funktionen, bei denen Einträge dieses Typs aufgelistet werden.

So wenden Sie den Gerätefilter an:

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Geräte**.
   Die **Geräte** Ansicht wird angezeigt.
2. Klicken Sie auf die **Filter** Schaltfläche (Lupensymbol) im Header der Web-Konsole.
   Der **Gerätefilter** Dialog wird mit dem Status **Es ist kein Filter aktiv** angezeigt.

3. Im **Gerätefilter** Dialog können Sie die folgenden Filteroptionen auswählen:

Option	Beschreibung
Name	Nach Gerätename filtern. Sie können einen Gerätenamen oder Teil eines Gerätenamens eingeben.
IMEI	Nach IMEI filtern.
Telefonnummer	Nach Telefonnummer filtern.
Managed	Wählen Sie **Ja**, um nur Geräte anzuzeigen, die provisioniert wurden. Wählen Sie **Nein**, um nur Geräte anzuzeigen, die nicht provisioniert wurden.
Compliant	Wählen Sie **Ja**, um nur Geräte anzuzeigen, die den Compliance-Richtlinien entsprechen. Wählen Sie **Ja**, um nur Geräte anzuzeigen, die den Compliance-Richtlinien nicht entsprechen.
Besitzer	Nach Besitzer filtern. Wählen Sie **Firmengerät** oder **Privates Gerät**.
Gerät zurückgesetzt	Wählen Sie **Ja**, um alle zurückgesetzten Geräte anzuzeigen. Wählen Sie **Nicht zurückgesetzt**, um alle nicht zurückgesetzten Geräte anzuzeigen.
Exchange Active Sync	Wählen Sie **Erlaubt**, um alle Geräte anzuzeigen, für die der E-Mail-Zugriff zugelassen ist. Wählen Sie **Erlaubt**, um alle Geräte anzuzeigen, für die der E-Mail-Zugriff nicht zugelassen ist. **Hinweis:** Die Steuerung des Zugriffs auf Unternehmens-E-Mails wird in Sophos Mobile Control as a Service nicht unterstützt. Wenn Sie Sophos Mobile Control as a Service benutzen, wird die Spalte **Exchange Active Sync** nicht angezeigt..
Softwarepaket	Nach Softwarepaket filtern. Geben Sie in den Feldern **Name**, **Kennung** und **Version** die Details für das relevante Softwarepaket ein. Wählen Sie in der Dropdownliste **Installiert**, um alle Geräte anzuzeigen, auf denen das Paket installiert ist. Wählen Sie **Nicht installiert**, um alle Geräte anzuzeigen, auf denen das Paket nicht installiert ist.
Gerätegruppe	Nach Gerätegruppen, denen die Geräte zugewiesen sind, filtern.
Betriebssystem	Nach Betriebssystem filtern. Hier können Sie Geräte mit einem bestimmten Betriebssystem abwählen.
Geräteeigenschaft	Nach spezifischer Geräteeigenschaft filtern. Geben Sie den **Namen** und den **Wert** der Geräteeigenschaft ein.

4. Wenn Sie die erforderlichen Kriterien ausgewählt haben, klicken Sie auf **Filtern**.

Der Filter wird aktiviert und die Geräteliste wird neu geladen. Die **Filter** Schaltfläche im Header der Web-Konsole ändert ihre Farbe von Blau zu Pink. Daduch wird angezeigt, dass der Filter aktiv ist. Für das Zurücksetzen des Filters wird im Header die **Aufheben** Schaltfläche angezeigt. Der Status des Gerätefilters im **Gerätefilter** Dialog ändert sich zu **Es ist ein Filter aktiv**.

Hinweis: Denken Sie daran, Filter manuell wieder aufzuheben, wenn sie nicht mehr benötigt werden. Andernfalls enthalten Listen oder Berichte unter Umständen nicht die erwarteten Ergebnisse.

21.2.2 Anwenden des Gerätegruppenfilters

Mit dem Gerätegruppenfilter können Sie die in Gerätegruppenlisten angezeigten Einträge einschränken.

Hinweis: Die Filter gelten nicht nur für die derzeit angezeigte Funktion, sondern für alle Funktionen, bei denen Einträge dieses Typs aufgelistet werden.

So wenden Sie den Gerätegruppenfilter an:

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Gerätegruppen**.

   Die **Gerätegruppen** Ansicht wird angezeigt.

2. Klicken Sie auf die **Filter** Schaltfläche (Lupensymbol) im Header der Web-Konsole.

   Der **Gruppenfilter** Dialog wird mit dem Status **Es ist kein Filter aktiv** angezeigt.

3. Geben Sie den **Namen** der Gerätegruppe ein und klicken Sie auf **Filtern**.

Der Filter wird aktiviert und die Gerätegruppenliste wird neu geladen. Die **Filter** Schaltfläche im Header der Web-Konsole ändert ihre Farbe von Blau zu Pink. Daduch wird angezeigt, dass der Filter aktiv ist. Für das Zurücksetzen des Filters wird im Header die **Aufheben** Schaltfläche angezeigt. Der Status des Gerätegruppenfilters im **Gruppenfilter** Dialog ändert sich zu **Es ist ein Filter aktiv**.

Hinweis: Denken Sie daran, Filter manuell wieder aufzuheben, wenn sie nicht mehr benötigt werden. Andernfalls enthalten Listen oder Berichte unter Umständen nicht die erwarteten Ergebnisse.

21.3 Bearbeiten von Geräten

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Geräte**.

   Die **Geräte** Ansicht mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, wird angezeigt.

2. Klicken Sie beim gewünschten Gerät auf das **Bearbeiten** Bleistiftsymbol.

   Die **Gerät bearbeiten** Ansicht für das ausgewählte Gerät wird angezeigt.

3. Nehmen Sie die notwendigen Änderungen vor (zum Beispiel in der **Installierte Software**Registerkarte Software installieren oder entfernen). Klicken Sie dann auf die **Speichern** Schaltfläche.

Ihre Änderungen werden auf das bearbeitete Gerät angewendet.

Hinweis: An Eigenschaften vorgenommene Änderungen treten erst in Kraft, wenn Sie auf **Speichern** geklickt haben. Wenn Sie die vorgenommenen Änderungen nicht speichern, haben sie keinerlei Auswirkungen.

21.3.1 Hinzufügen einer LDAP-Verknüpfung zum Gerät

Wenn Sie ein Gerät auf der Grundlage einer Vorlage erstellen oder ein Gerät bearbeiten, können Sie eine LDAP-Verknüpfung zu einzelnen Geräten hinzufügen.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Geräte**.

   Die **Geräte** Ansicht mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, wird angezeigt.

2. Klicken Sie beim gewünschten Gerät auf das **Bearbeiten** Bleistiftsymbol.

   Die **Gerät bearbeiten** Ansicht für das ausgewählte Gerät wird angezeigt.

3. Klicken Sie auf die **LDAP-Verknüpfung setzen** Schaltfläche.

   Die **LDAP-Suchparameter eingeben** Ansicht wird angezeigt.

4. Geben Sie in den Felder **Verzeichnis-Server**, **Basisknoten**, **Common Name** (**CN**) und **E-Mail-Adresse** die erforderlichen Suchkriterien ein und klicken Sie auf **Weiter**.

   Die **Datensatz wählen** Ansicht wird angezeigt.

5. Wählen Sie den gewünschten Datensatz aus und klicken Sie auf **Weiter**.

   Die **Detailfelder wählen** Ansicht wird angezeigt.

6. Wählen Sie die erforderliche **E-Mail-Adresse** und den **Benutzernamen** aus und klicken Sie auf **Übernehmen**.

   Die **Gerät bearbeiten** Ansicht wird wieder angezeigt.

7. Klicken Sie auf die **Speichern** Schaltfläche.

Hinweis: Das Gerät wird für den relevanten Benutzer im Self Service Portal angezeigt.

21.3.2 Definieren eigener Eigenschaften für Geräte

Wenn Sie ein Gerät auf der Grundlage einer Vorlage erstellen oder ein Gerät bearbeiten, können Sie eigene Eigenschaften definieren, zum Beispiel Systemprozesse.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Geräte**.

   Die **Geräte** Ansicht mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, wird angezeigt.

2. Klicken Sie beim gewünschten Gerät auf das **Bearbeiten** Bleistiftsymbol.

   Die **Gerät bearbeiten** Ansicht für das ausgewählte Gerät wird angezeigt.

3. Wechseln Sie in die **Eigene Eigenschaften** Registerkarte und klicken Sie auf die **Neue Eigenschaft anlegen** Schaltfläche.

   Die **Eigenschaft bearbeiten** Ansicht wird angezeigt.

4. Geben Sie einen **Namen** und einen **Wert** für die neue eigene Eigenschaft ein.

   Zum Beispiel für Systemprozesse:

   - Name: SystemProcess2
   - Value: Internet;10008d39,BrowserNG.exe

   Für Systemprozesse lautet der **Name** immer "SystemProcess" gefolgt von einem bei "0" beginnenden Index. Leerzeichen sind nicht zulässig. Wenn Sie einen weiteren Prozess anlegen, verwenden Sie den folgenden Index, zum Beispiel "SystemProcess1", "SystemProcess2" usw.

   Die Syntax für **Wert** lautet: <Anzeigename>;<UID des Prozesses <Name des Prozesses>.

   Sie können auch mehrere Prozesse kombinieren, zum Beispiel: <Anzeigename>;<UID des Prozesses>,<Name des Prozesses>;<UID des Prozesses>,<Name des Prozesses>.

5. Klicken Sie auf die **Übernehmen** Schaltfläche.

   Die neue Eigenschaft wird in der **Gerät bearbeiten** Ansicht in der **Eigene Eigenschaften** Registerkarte angezeigt.

6. Klicken Sie auf die **Speichern** Schaltfläche.

21.4 Ausführen von administrativen Aufgaben

Die Web-Konsole bietet eine Reihe von Funktionsschaltflächen für administrative Aufgaben in den Ansichten **Gerät anzeigen** und **Gerät bearbeiten**.

Um bei einem einzelnen Gerät Aufgaben auszuführen, öffnen Sie die **Gerät anzeigen** oder die **Gerät bearbeiten** Ansicht für das gewünschte Gerät (siehe *Einsehen von Geräten* (Seite 91) and *Bearbeiten von Geräten* (Seite 96)) und klicken Sie auf die Funktionsschaltfläche für die gewünschte Aufgabe.

Hinweis: Die verfügbaren Funktionsschaltflächen richten sich nach Mobilgerätetyp (Plattform), Konfiguration und Geräteansicht (**Gerät zeigen** oder **Gerät bearbeiten**).

Schaltfläche	Beschreibung
	Klicken Sie auf diese Schaltfläche, um den Namen und die IMEI eines spezifischen Geräts im Gerätefilter einzustellen, siehe *Anwenden des Gerätefilters* (Seite 93).
	Klicken Sie auf diese Schaltfläche, um alle Aufträge für dieses Gerät abzurufen.

Schaltfläche	Beschreibung
	Diese Schaltfläche steht für Geräte zur Verfügung, bei denen die Registrierung über das Self Service Portal fehlgeschlagen ist. Klicken Sie auf diese Schaltfläche, um den Status der fehlgeschlagenen SSP-Registrierung zurückzusetzen, nachdem Sie die relevanten Probleme behoben haben. **Hinweis:** Verwenden Sie diese Schaltfläche nur dann, wenn Sie sicher sind, dass sich das Gerät trotzdem mit dem Sophos Mobile Control Server synchronisiert.
	Klicken Sie auf diese Schaltfläche, um eine ActiveDirectory-Verbindung zum Gerät hinzuzufügen.
	Klicken Sie auf diese Schaltfläche, um eine ActiveDirectory-Verbindung zum Gerät zu entfernen.
	Klicken Sie auf diese Schaltfläche, um die Gerätedaten zu aktualisieren.
	Klicken Sie auf diese Schaltfläche, um den Datenzähler für das Gerät zu öffnen, siehe *Einsehen des Datenverkehrs mit dem Datenzähler* (Seite 110).
	Gibt an, dass der E-Mail-Zugriff verweigert wird. Ein zusätzliches Symbol auf der Schaltfläche gibt an, ob der E-Mail-Zugriff ■ manuell oder ■ automatisch zugelassen wurde. Klicken Sie auf dieser Schaltfläche, um den E-Mail-Zugriff zuzulassen oder auf in den automatischen Modus zu setzen. **Hinweis:** Die Steuerung des Zugriffs auf Unternehmens-E-Mails wird in Sophos Mobile Control as a Service nicht unterstützt. Wenn Sie Sophos Mobile Control as a Service benutzen, wird diese Schaltfläche nicht angezeigt.
	Gibt an, dass der E-Mail-Zugriff zugelassen wird. Ein zusätzliches Symbol auf der Schaltfläche gibt an, ob der E-Mail-Zugriff ■ manuell oder ■ automatisch zugelassen wurde.

Schaltfläche	Beschreibung
	Klicken Sie auf diese Schaltfläche, um den E-Mail-Zugriff zu verweigern oder auf in den automatischen Modus zu setzen. **Hinweis:** Die Steuerung des Zugriffs auf Unternehmens-E-Mails wird in Sophos Mobile Control as a Service nicht unterstützt. Wenn Sie Sophos Mobile Control as a Service benutzen, wird diese Schaltfläche nicht angezeigt.
	Gibt an, dass die Active Sync ID für das Gerät unbekannt ist. Einstellungen haben keine Auswirkungen. Wie eine Active Sync ID für ein Gerät ermittelt wird, hängt vom Gerätetyp ab: ■ Für Apple iOS und Windows Mobile Geräte ist die Active Sync ID bekannt, sobald das Gerät durch das SMC Profil/den SMC Client verwaltet wird. ■ Für Android-Geräte wird die ID aufgelöst, wenn sich das Gerät zum ersten Mal mit dem Exchange Server verbindet. Geräte werden anhand Ihres Exchange-Benutzernamens identifiziert. Die Active Sync ID wird dann eingetragen. **Hinweis:** Dies ist nur dann möglich, wenn nur ein Gerät gefunden wird. **Hinweis:** Die Steuerung des Zugriffs auf Unternehmens-E-Mails wird in Sophos Mobile Control as a Service nicht unterstützt. Wenn Sie Sophos Mobile Control as a Service benutzen, wird diese Schaltfläche nicht angezeigt.
	Klicken Sie auf diese Schaltfläche, um das Gerät remote zu sperren.
	Klicken Sie auf diese Schaltfläche, um den Passcode/das Passwort eines Geräts zurückzusetzen. ■ Für Apple IOS Geräte wird der Passcode/das Passwort auf dem Gerät zurückgesetzt und der Benutzer wird dazu aufgefordert, einen neuen Passcode/ein neues Passwort zu definieren. ■ Für Android Geräte können Sie den alten Passcode/das alte Passwort ersetzen. Der neue Passcode/das neue Passwort muss den Passcode-/Kennwortregeln entsprechen.
	Klicken Sie auf diese Schaltfläche, um alle Synchronisierungsdaten des Geräts zu löschen. Der Sophos Mobile Control Client muss neu installiert werden.

Schaltfläche	Beschreibung
	Klicken Sie auf diese Schaltfläche, um das Gerät bei Verlust oder Diebstahl auf den Werkszustand zurückzusetzen (Wipe). Das Gerät wird auf den Werkszustand zurückgesetzt. Alle Daten werden gelöscht.
	Klicken Sie auf diese Schaltfläche, um eine benutzerdefinierte Nachricht an ein spezifisches Gerät zu senden. Nach dem Bootstrap eines iOS-Geräts und der Installation der Sophos Mobile Control App werden APNs-Nachrichten gesendet. Nach dem Einrichten eines Android-Geräts werden GCM Push-Nachrichten gesendet.
	Klicken Sie auf diese Schaltfläche, um ein iOS- oder Android-Gerät zu orten.
	Klicken Sie auf diese Schaltfläche, um die Gerätedaten aus einem Backup wiederherzustellen. Für weitere Informationen zu Backups siehe *Geräte-Backups* (Seite 111). **Hinweis:** Diese Option ist nur für Android und Windows Mobile Geräte verfügbar. Backups werden für Sophos Mobile Control as a Service nicht unterstützt.
	Klicken Sie auf diese Schaltfläche, um das Gerät zu löschen. **Hinweis:** Wenn Sie ein Gerät löschen, werden automatisch auch dessen Aufträge gelöscht. Der Server löscht alles, was mit dem Gerät in Verbindung steht, auch synchronisierte Informationen. Der Löschvorgang auf Server-Seite hat keine Auswirkungen auf die Client-Seite. Wenn Sie den Client deinstallieren müssen, müssen Sie den Sophos Mobile Control Client manuell entfernen.
	Klicken Sie auf diese Schaltfläche, um die Sophos Mobile Control App nach der Installation auf einem iOS-Gerät zu aktivieren. Dies ist ein notwendiger Schritte für das Einrichten von Sophos Mobile Control auf Apple iOS Geräten. Um sicherzustellen, dass die Aktivierung funktioniert, muss die App zuvor einmal auf dem Gerät geöffnet werden.
	Klicken Sie auf diese Schaltfläche, um ein iOS- oder Android-Gerät zu deregistrieren, siehe *Deregistrieren von Geräten* (Seite 102). **Hinweis:** Diese Option ist nur für Android-Geräte und Apple iOS Geräte verfügbar.
	Diese Schaltfläche ist verfügbar, wenn Sie eine Lizenz zum Verwalten der Sophos Mobile Security App von der Sophos Mobile Control Web-Konsole aus haben. Für weitere Informationen siehe *Verwaltung von Sophos Mobile Security über Sophos Mobile Control* (Seite 114). Klicken Sie auf diese Schaltfläche, um einen Sophos Mobile Security Scan auf einem bestimmten Gerät zu starten.

Hinweis: An Eigenschaften vorgenommene Änderungen treten erst in Kraft, wenn Sie auf **Speichern** geklickt haben. Wenn Sie die vorgenommenen Änderungen nicht speichern, haben sie keinerlei Auswirkungen.

21.5 Deregistrieren von Geräten

Sie können durch Sophos Mobile Control verwaltete Android- und iOS-Geräte deregistrieren, wenn sie nicht mehr benutzt werden, weil der Benutzer zum Beispiel ein neues Gerät erhält. Dies ist zum Beispiel nützlich, wenn Sie die Anzahl an Geräten, die ein Benutzer über das Self Service Portal registrieren kann, begrenzt haben.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Geräte**.

   Die **Geräte** Ansicht mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, wird angezeigt.

2. Klicken Sie beim gewünschten Gerät auf das **Bearbeiten** Bleistiftsymbol.

   Die **Gerät bearbeiten** Ansicht für das ausgewählte Gerät wird angezeigt.

3. Klicken Sie auf die **Gerät deregistrieren** Schaltfläche.

   Eine Meldung wird angezeigt, die Sie zur Bestätigung des Deregistrierungsvorgangs auffordert.

4. Klicken Sie auf **Ja**.

Das Gerät wird deregistriert. Dadurch werden folgende Vorgänge ausgelöst:

Android-Geräte:

- Der Sophos Mobile Control Geräteadministrator wird deaktiviert.
- Die Server-Anmeldedaten und alle weiteren erhaltenen Daten werden entfernt.

Apple iOS-Geräte:

- Alle Profile werden entfernt.
- Alle Managed Apps werden entfernt (ab iOS 5.1).
- Die Sophos Mobile Control iOS Client App wird entfernt, falls Sie über Managed Apps (ab iOS 5.1) installiert wurde.
- Alle über Mobile Device Management erhaltenen Zertifikate werden entfernt.

21.6 Gerätegruppen

Gerätegruppen dienen zur Kategorisierung von Geräten. Sie können Geräte zu Gerätegruppen zuweisen, wenn Sie sie zum Sophos Mobile Control Device Management manuell oder über Import hinzufügen. Die Gerätegruppe für ein Gerät lässt sich durch Bearbeiten des Geräts ändern. Ein Gerät gehört jeweils immer exakt zu einer Gerätegruppe. Gerätegruppen vereinfachen die Verwaltung von Geräten, da in den meisten Device Management Funktionen entweder eine komplette Gruppe oder Einzelgeräte ausgewählt werden können.

Hinweis: Wir empfehlen, nur Geräte mit demselben Betriebssystem zu gruppieren. Gruppen lassen sich dadurch leichter für Installationen und andere betriebssystemspezifische Vorgänge verwenden.

Für weitere Informationen zum Erstellen von Gerätegruppen, siehe *Erstellen von Gerätegruppen* (Seite 36).

Hinweis: Wenn Sie eine Gerätegruppe löschen, werden die Mitglieder der Gruppe in eine andere Gruppe verschoben. Diese muss angegeben werden. Ist keine Gruppe mehr vorhanden, in die die Geräte verschoben werden können, so kann die Gruppe nicht gelöscht werden. Bevor eine Gruppe gelöscht wird, wird eine Warnungsmeldung angezeigt.

22 Einsehen von Aufträgen in der Web-Konsole

Sie können alle vorhandenen Aufträge für Geräte in der Web-Konsole überwachen:

- Die **Auftragsstatus** Ansicht zeigt alle noch nicht abgeschlossenen und fehlgeschlagenen Aufträge sowie die abgeschlossenen Aufträge der letzten paar Tage. Die **Auftragsstatus** Ansicht wird automatisch aktualisiert. Sie können somit den Fortschritt der Aufträge verfolgen.
- Die **Auftragshistorie** zeigt allgemeine Informationen zu einem Auftrag aus der **Auftragsstatus** oder der **Auftragsarchiv** Ansicht.
- Das **Auftragsarchiv** zeigt alle Aufträge.

22.1 Einsehen von nicht abgeschlossenen, fehlgeschlagenen und zuletzt abgeschlossenen Aufträgen

1. Klicken Sie in der Web-Konsolen-Menüleiste auf **Auftragsstatus**.

   Die **Auftragsstatus** Ansicht wird angezeigt. Die **Status** Spalte zeigt den Auftragsstatus, zum Beispiel **Endgültig fehlgeschlagen**.

2. Im Feld **Aktualisierungsintervall (in Sek.)** können Sie auswählen, wie oft der **Auftragsstatus** aktualisiert werden soll.
3. Um weitere Details zu einem Auftrag einzusehen, klicken Sie auf das **Anzeigen** Lupensymbol neben den gewünschten Auftrag.

   Die **Auftragshistorie** Ansicht wird angezeigt. Neben allgemeinen Informationen zum Auftrag (z. B. **Gerät**, **Paketname**, **Erstellt** usw.) zeigt die Auftragshistorie die Status, die ein bestimmter Auftrag durchlaufen hat, mit Zeitstempeln und Fehlercodes. Wenn Kommandos vom Gerät auszuführen sind, wird in der **Auftragshistorie** zusätzlich eine **Details** Schaltfläche angezeigt.

4. Klicken Sie auf die **Details** Schaltfläche, falls verfügbar, um das vom Gerät auszuführende Kommando einzusehen.

   Die **Kommandos** Ansicht mit den relevanten Kommandos wird angezeigt. Die an das Gerät geschickten Kommandos sind Teil des Auftrags. Sie werden vom Client ausgeführt. Die Ergebnisse, die Erfolg oder Fehlschlag angeben, werden an den Server zurück gesendet. Ist kein Fehler aufgetreten, so lautet der Fehlercode "0". Ist ein Kommando fehlgeschlagen, so wird der entsprechende Fehlercode angezeigt. Meistens werden auch Informationen dazu angezeigt, was den Fehlschlag verursacht haben könnte.

5. Um in die **Auftragshistorie** Ansicht zurückzukehren, klicken Sie auf die **Zurück** Schaltfläche.
6. Um fehlgeschlagene Aufträge manuell erneut auszuführen, klicken Sie auf die **Jetzt ausführen** Schaltfläche.

   Hinweis: Diese Schaltfläche wird nur für fehlgeschlagene Aufträge angezeigt. Sie können nur Aufträge erneut ausführen, die noch nicht vollständig fehlgeschlagen sind.

22.2 Einsehen des Auftragsarchivs

1. Klicken Sie in der Web-Konsolen-Menüleiste auf **Auftragsarchiv**.

   Die **Auftragsarchiv** Ansicht wird angezeigt. Sie zeigt alle abgeschlossenen und fehlgeschlagenen Aufträge im System.

2. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Klicken Sie auf die **Neu laden** Schaltfläche, um die **Auftragsarchiv** Ansicht zu aktualisieren.
   - Wählen Sie Aufträge aus und klicken Sie auf die **Gewählte löschen** Schaltfläche, um sie aus dem Archiv zu löschen.

22.3 Anwenden des Auftragsfilters

Mit Filtern lässt sich die Anzahl an in Listen angezeigten Einträgen nach definierten Kriterien einschränken. Mit dem Auftragsfilter können Sie die in der Auftragsstatus- und in der Auftragsarchiv-Ansicht angezeigten Aufträge filtern.

Hinweis: Die Filter gelten nicht nur für die derzeit angezeigte Funktion, sondern für alle Funktionen, bei denen Einträge dieses Typs aufgelistet werden.

So wenden Sie den Auftragsfilter an:

1. Klicken Sie in der Web-Konsolen-Menüleiste auf **Auftragsstatus** oder **Auftragsarchiv**.

   Die **Auftragsstatus/Auftragsarchiv** Ansicht wird angezeigt.

2. Klicken Sie auf die **Filter** Schaltfläche (Lupensymbol) im Header der Web-Konsole.

   Der **Auftragsfilter** Dialog wird mit dem Status **Es ist kein Filter aktiv** angezeigt.

3. Im **Auftragsfilter** Dialog können Sie die folgenden Filteroptionen auswählen:

Option	Beschreibung
Gerät	Nach Gerätename filtern.
Softwarepaket	Nach Paketname filtern.
Erstellt von	Nach dem Namen des Benutzers, der die Aufträge erstellt hat, filtern.
Status	Nach Auftragsstatus filtern. Sie können folgende Status auswählen: ■ **Geplant** ■ **In Bearbeitung** ■ **Erfolgreich** ■ **Fehlgeschlagen**
Gruppe	Nach Gerätegruppe filtern.

4. Wenn Sie die erforderlichen Kriterien ausgewählt haben, klicken Sie auf **Filtern**.

Der Filter wird aktiviert und die Geräteliste wird neu geladen. Die **Filter** Schaltfläche im Header der Web-Konsole ändert ihre Farbe von Blau zu Pink. Dadurch wird angezeigt, dass der Filter aktiv ist. Für das Zurücksetzen des Filters wird im Header die **Aufheben** Schaltfläche angezeigt. Der Status des Auftragsfilters im **Auftragsfilter** Dialog ändert sich zu **Es ist ein Filter aktiv**. Im Dialog steht eine **Aufheben** Schaltfläche zum Zurücksetzen des Filters zur Verfügung.

Hinweis: Denken Sie daran, Filter manuell wieder aufzuheben, wenn sie nicht mehr benötigt werden. Andernfalls enthalten Listen oder Berichte unter Umständen nicht die erwarteten Ergebnisse.

22.4 Auftragssymbole

In der **Auftragsstatus** Ansicht und im **Auftragsarchiv** werden Symbole zur Kategorisierung der angezeigten Aufträge verwendet. Die Symbole haben folgende Bedeutung:

Symbol	Beschreibung
	Installation
	Deinstallation
	Prozessaktivierung/-deaktivierung

Symbol	Beschreibung
	Explizite Aktualisierung von Gerätedaten
	Nachricht an das Gerät
	Windows Mobile Profil-Transfer
	IOS Profil-Transfer
	Kommandopaket-Transfer
	Auftragspaket-Transfer
	Bootstrap
	Kommando-Transfer
	Windows Mobile Sicherheitseinstellungen

22.5 Auftragsstatus

Die folgende Tabelle bietet einen Überblick zu den in der **Auftragsstatus** Ansicht und im **Auftragsarchiv** angezeigten Auftragsstatus.

Farbsymbol	Status	Beschreibung
●	Angenommen	Der Auftrag wurde erstellt.
●	Wiederholung	Der Auftrag wird später wiederholt.
●	Gestartet	Der Auftrag wurde gestartet.
●	In Bearbeitung	Die Ausführung des Auftrags wird vorbereitet.
●	Sende Benachrichtigung	Der Client wird benachrichtigt
●	Warte auf Zustellung	Der Server wartet auf die Bestätigung der Benachrichtigung durch den Client.
●	Benachrichtigung	Der Client hat die Benachrichtigung erhalten.
●	Ausgeliefert	Der Client hat das Paket bzw. die Kommandos erhalten.

Farbsymbol	Status	Beschreibung
	Ergebnisauswertung gestartet.	Der Client hat geantwortet und die Auswertung des Ergebnisses wurde gestartet.
	Ergebnis unvollständig	Die Ergebnisauswertung hat gezeigt, dass nicht alle Ergebnisse des Kommandos eingegangen sind.
	Erfolgreich	Das Paket wurde installiert oder die Kommandos wurden erfolgreich ausgeführt. **Hinweis:** Für die Ersteinrichtung (Provisionierung) des Sophos Mobile Control Client muss der Auftrag mit dem Status "Installiert " abgeschlossen werden.
	Installiert	Der Sophos Mobile Control Client wurde erfolgreich installiert. Das Gerät ist nun provisioniert.
	Ergebnisauswertung fehlgeschlagen	Die Ergebnisauswertung konnte nicht durchgeführt werden.
	Auftrag teilweise fehlgeschlagen	Nicht alle Kommandos des Auftrags konnten erfolgreich ausgeführt werden.
	Verschoben	Der Auftrag wird später neu gestartet.
	Fehlgeschlagen (wird wiederholt)	Der Auftrag ist fehlgeschlagen und wird später wiederholt.
	Auftrag fehlgeschlagen	Der Auftrag ist fehlgeschlagen und wird nicht wiederholt.
	Endgültig fehlgeschlagen	Der Auftrag ist fehlgeschlagen.

23 Berichte

Die Sophos Mobile Control Web-Konsole bietet verschiedene Arten von Berichten:

- Graphischer Bericht, der einen Überblick zu registrierten Berichten liefert. Dieser Bericht wird in der **Reports** Ansicht in der Web-Konsole angezeigt.
- Bericht mit detaillierten Informationen zu Geräten Dieser Bericht wird in eine .csv-Datei exportiert.
- **Datenzähler**, der die im laufenden und vorigen Monat übertragenen Datenmengen zeigt.

  Hinweis: Der **Datenzähler** ist nur für Android-Geräte und Windows Mobile Geräte verfügbar.

23.1 Erstellen eines graphischen Berichts zu Geräten

Sie können einen graphischen Bericht zu Geräten erstellen, der statistische Informationen zu den registrierten Geräten für den relevanten Kunden in Tortendiagrammen zeigt.

1. Klicken Sie in der **Startseite** Ansicht auf die **Reports** Schaltfläche.

Die **Reports** Ansicht wird angezeigt. Diese Ansicht zeigt die folgenden Informationen in Tortendiagrammen:

- Geräte, die compliant/nicht compliant sind.
- Geräte, die managed/nicht managed sind.
- Firmengeräte/private Geräte
- Geräte nach Betriebssystemtyp
- Geräte nach Betriebssystemversion pro Betriebssystemtyp

23.2 Exportieren von Geräteinformationen in eine CSV-Datei

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Geräte**.

   Die **Geräte** Ansicht wird angezeigt.

2. Klicken Sie auf die **Auswertung erstellen** (**CSV-Datei**) Schaltfläche.

   Ein Dialog für den Datei-Download wird angezeigt.

3. Wählen Sie einen Speicherort aus und klicken Sie auf **Speichern**.

Der Bericht wird in einer .csv-Datei am angegebenen Speicherort gespeichert.

Hinweis: Im Bericht werden etwaig gesetzte Filter berücksichtigt. Wenn der Bericht nicht die erwarteten Ergebnisse liefert, überprüfen Sie die aktuellen Filter.

Hinweis: Das Geräteberichtsformat unterscheidet sich vom Geräteimport-Tabellenformat. Es enthält wesentlich mehr Informationen. Eine exportierte Liste kann daher nur nach

umfangreichen Anpassungen importiert werden. Für weitere Informationen siehe *Importieren von Geräten* (Seite 38).

23.3 Einsehen des Datenverkehrs mit dem Datenzähler

Hinweis: Der **Datenzähler** ist nur für Android-Geräte und Windows Mobile Geräte verfügbar.

Im **Datenzähler** werden die im laufenden und vorigen Monat übertragenen Datenmengen angezeigt. Der Datenzähler gibt einen groben Überblick über alle Geräte. Wenn ein Gerät ein konfiguriertes Limit erreicht, sendet der Server eine SMS oder eine Warnmeldung.

Hinweis: Der **Datenzähler** schränkt die Datenübertragungsmenge nicht ein, auch dann nicht, wenn das Limit erreicht ist. Es informiert lediglich den Benutzer des Geräts.

1. Klicken Sie in der Web-Konsolen-Menüleiste auf **Datenzähler**.

   Die **Datenzähler** Ansicht wird angezeigt. Sie zeigt einen Überblick zu den übertragenen Datenmengen für alle registrierten Geräte für den laufenden und den vorigen Monat.

   Hinweis: In der **Datenzähler** Ansicht werden bei Datenübertragung bestimmte Werte rot markiert. Dadurch wird ein besserer Überblick zu gewünschtem oder nicht gewünschtem Datenverkehr geboten. Wi-Fi-Datenverkehr wird daher nie rot markiert. GSM-Datenverkehr wird nur dann rot markiert, wenn das Limit überschritten wird. GSM Roaming-Datenverkehr wird sofort beim Auftreten rot markiert.

2. Um die Datenzählerdetails für ein bestimmtes Gerät einzusehen, klicken Sie in der **Datenzähler** Ansicht auf das gewünschte Gerät.

   Die **Datenzählerdetails anzeigen** Ansicht wird angezeigt. Sie zeigt allgemeine Informationen sowie eine jährliche Übersicht für das ausgewählte Gerät.

3. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Wählen Sie zwischen verschiedenen Datenverkehrstypen, um die Anzeige entsprechend einzuschränken:
     - **Zeige WiFi**
     - **Zeige GSM**
     - **Zeige GSM-Roaming**

     Klicken Sie auf **Aktualisieren**, um die Anzeige entsprechend zu aktualisieren.
   - Klicken Sie unter **Jahresübersicht** auf einen Monat, um die Daten für den ausgewählten Monat abzurufen.

24 Geräte-Backups

Hinweis: Die Backup-Konfiguration ist nur für Android und Windows Mobile Geräte verfügbar. Die Backup-Konfiguration wird für Sophos Mobile Control as a Service nicht unterstützt.

Sie können Backups für Geräte konfigurieren, um SMS, Lesezeichen und benutzerdefinierte Verzeichnispfade zu sichern.

Hinweis: Backups sind plattformspezifisch.

24.1 Konfigurieren von Geräte-Backups

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Backup** auf **Profile**.

   Die **Backup-Konfigurationen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neues Paket anlegen**.

   Die **Backup-Konfiguration bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Version** für die neue Backup-Konfiguration ein.
4. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das die Backup-Konfiguration gelten soll.
5. Wählen Sie unter **Zeitplan** die Wochentage und die Uhrzeit für die Backup-Erstellung aus.
6. Wählen Sie die Komponenten aus, die in den Backup einbezogen werden sollen:

   a) Wählen Sie **SMS**, um Textnachrichten einzubeziehen.

   b) Wählen Sie **Lesezeichen des Systembrowsers**, um Lesezeichen einzubeziehen.

   c) Klicken Sie unter **Zu sichernde Pfade** auf die **Pfad hinzufügen** Schaltfläche.

      Die **Pfad** Ansicht wird angezeigt.

   d) Geben Sie in der **Pfad** Ansicht einen Pfad ein, der in den Backup einbezogen werden soll, zum Beispiel /files/. Falls erforderlich, wählen Sie **Rekursiv**.

   e) Geben Sie unter **Zu sichernde Dateien (Wildcard * erlaubt)** die Dateien ein, die in den Backup einbezogen werden sollen. Klicken Sie dann auf **Hinzufügen**.

      Die Dateien werden im Text-Feld unten angezeigt.

   f) Klicken Sie auf die **Speichern** Schaltfläche.

      Der angegebene Pfad wird unter **Zu sichernde Pfade** in der **Backup-Konfiguration bearbeiten** Ansicht angezeigt.

7. Klicken Sie auf die **Speichern** Schaltfläche.

Die neue Backup-Konfiguration wird unter **Backup-Konfigurationen** angezeigt. Sie können sie nun an Geräte oder Gerätegruppen übertragen.

24.2 Übertragen von Backup-Konfigurationen

Um sicherzustellen, dass Backups von Geräten erstellt werden, müssen Sie die erstellten Backup-Konfigurationen an Geräte oder Gerätegruppen übertragen.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Backup** auf **Übertragung**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

2. Der nächste Schritt hängt davon ab, ob Sie die Konfiguration an einzelne Geräte oder Gerätegruppen übertragen möchten:

   - Wenn Sie die Konfiguration an einzelne Geräte übertragen möchten, wählen Sie die gewünschten Geräte in der **Gerät(e) wählen** Ansicht aus und klicken Sie auf **Weiter**.
   - Wenn Sie die Konfiguration an Gerätegruppen übertragen möchten, klicken Sie auf die **Gruppenauswahl** Schaltfläche, wählen Sie die gewünschte(n) Gruppe(n) in der **Gerätegruppe(n) wählen** Ansicht aus und klicken Sie auf **Weiter**.

   Die **Backup-Konfiguration wählen** Ansicht wird angezeigt.

3. Wählen Sie die Backup-Konfiguration aus, die Sie übertragen möchten, und klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

4. Geben Sie ein **Auftragsdatum** für die Übertragung der Backup-Konfiguration an.
5. Klicken Sie auf die **Fertigstellen** Schaltfläche.

Die Backup-Konfiguration wird an die ausgewählten Geräte oder Gerätegruppen zur angegebenen Ausführungszeit übertragen.

24.3 Wiederherstellen von Daten aus Backups

1. Klicken Sie in der Web-Konsole unter **Inventar** auf **Geräte**.
2. Die **Geräte** Ansicht wird angezeigt.
3. Klicken Sie auf das **Anzeigen** oder **Bearbeiten** Symbol neben dem Gerät, für das Sie Daten aus einem Backup wiederherstellen möchten.

   Die **Gerät anzeigen/Gerät bearbeiten** Ansicht wird angezeigt.

4. Klicken Sie auf die **Daten aus Backup wiederherstellen** Schaltfläche.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

5. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
6. Klicken Sie auf die **Fertigstellen** Schaltfläche.

Die Daten werden aus dem Backup auf dem gewählten Gerät zum angegebenen Zeitpunkt wiederhergestellt.

25 Senden von Nachrichten an Geräte

Von der Web-Konsole aus können Sie benutzerdefinierte Nachrichten an verwaltete Geräte schicken. Nach dem Bootstrap eines iOS-Geräts und der Installation der Sophos Mobile Control App werden APNs-Nachrichten gesendet. Nach dem Einrichten eines Android-Geräts werden GCM Push-Nachrichten gesendet.

1. Klicken Sie in der Web-Konsolen-Menüleiste auf **Nachrichten**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

2. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Wählen Sie einzelne Geräte aus, an die die Nachricht gesendet werden soll.
   - Klicken Sie auf die **Gruppenauswahl** Schaltfläche, um die **Gerätegruppe(n) wählen** Ansicht zu öffnen. Wählen Sie dann ein oder mehrere Gerätegruppen für das Senden der Nachricht aus.

3. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Der Dialog **Mitteilungstext eingeben** wird angezeigt.

4. Geben Sie im Textfeld die gewünschte Mitteilung ein. Ein Zeichenzähler unterhalb des Textfelds zählt von der Gesamtanzahl an verfügbaren Zeichen auf 0. Wenn der Wert 0 erreicht ist, können Sie keine weiteren Zeichen mehr eingeben. Wenn Sie den Mitteilungstext eingegeben haben, klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

5. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
6. Klicken Sie auf die **Fertigstellen** Schaltfläche.

Die Nachricht wird zum angegebenen Zeitpunkt an die ausgewählten Geräte gesendet.

Hinweis: Sie können auch Nachrichten vom **Inventar** aus an Geräte senden. Für weitere Informationen siehe *Ausführen von administrativen Aufgaben* (Seite 98).

26 Verwaltung von Sophos Mobile Security über Sophos Mobile Control

Sophos Mobile Security ist eine Security App für Android-Mobiltelefone und Tablets, die Geräte vor schädlichen Apps schützt und Endbenutzer beim Erkennen von App-Berechtigungen unterstützt, die u. U. ein Sicherheitsrisiko darstellen.

Sophos Mobile Security Management ist ein optionales Modul von Sophos Mobile Control. Zum Verwalten der Sophos Mobile Security App von Sophos Mobile Control aus muss eine Lizenz verfügbar sein. Diese Lizenz muss in der Sophos Mobile Control Web-Konsole aktiviert werden.

So verwalten Sie die Sophos Mobile Security App auf Managed-Geräten über die Sophos Mobile Control Web-Konsole:

- Sie können Einstellungen für die Sophos Mobile Security App auf allen Managed-Endbenutzergeräten remote und zentral in der Web-Konsole konfigurieren.
- Sie können sicherstellen, dass die Sophos Mobile Security App auf Endbenutzergeräten installiert ist und in festgelegten Intervallen Scans durchführt. Sie können dies als Compliance-Kriterium definieren.
- Sie können Scans bei bestimmten Geräten auslösen.
- Sie können die Scan-Ergebnisse für Geräte in der Web-Konsole einsehen.

Weitere Informationen zu Sophos Mobile Security finden Sie in der *Sophos Mobile Security Hilfe*.

26.1 Lizenzen für die Verwaltung von Sophos Mobile Security

Für die Verwaltung der Sophos Mobile Security App über Sophos Mobile Control sind gültige Lizenzen erforderlich. Nach dem Erwerb erhalten Sie einen Lizenzschlüssel zur Aktivierung der Sophos Mobile Security Lizenz. Wie Sie die Lizenz in der Web-Konsole aktivieren, hängt von der verwendeten Sophos Mobile Control Variante (lokale Installation oder Software as a Service) ab.

26.1.1 Aktivierung von Lizenzen für lokale Installationen

Für lokale Sophos Mobile Control Installationen werden Sophos Mobile Security Lizenzen vom Superadministrator in der Kundenverwaltung verwaltet. Weitere Infomraitonen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

26.1.2 Aktivieren der Lizenz für Software as a Service Installationen

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Einstellungen**.

   Die **Einstellungen** Ansicht wird angezeigt.

2. Wechseln Sie in die **SMSec** Registerkarte.

3. Geben Sie im **Lizenzschlüssel** Feld den von Sophos erhaltenen Lizenzschlüssel ein und klicken Sie auf **Aktivieren**.

Der Sophos Mobile Control Lizenz wird aktiviert. Das **Aktiver Lizenzschlüssel** Feld zeigt den aktivierten Lizenzschlüssel. Das **Anzahl an Clients** Feld zeigt die Anzahl an verfügbaren Clients. Das **Gültig bis Feld** zeigt das Lizenzablaufdatum.

Auf der **Startseite** werden die Lizenzinformationen in der **SMSec** Zeile in den Feldern **Managed Geräte**, **Lizensierte Geräte** und **Lizenz gültig bis** angezeigt.

26.2 Konfigurieren von Einstellungen für Sophos Mobile Security

Voraussetzung: Es ist eine Lizenz für die Verwaltung von Sophos Mobile Security über die Sophos Mobile Control Web-Konsole verfügbar.

1. Klicken Sie in der **Startseite** Ansicht auf die Schaltfläche **Einstellungen**.

   Die **Einstellungen** Ansicht wird angezeigt.

2. Wechseln Sie in die **SMSec** Registerkarte.
3. Unter **Allgemein** können Sie folgende Einstellungen festlegen:

   a) Legen Sie im **Cloud Scan-Modus** Feld fest, wann Sophos Mobile Security einen Scan nach den aktuellen Malware-Informationen durchführen soll. Wählen Sie eine der folgenden Optionen, um festzulegen, wann die Anwendung eine Cloud-Abfrage nutzen soll:

   - **Immer**
   - **Nicht beim Roaming**
   - **Nur WLAN**

   Mit dieser Einstellung lässt sich der Datenverkehr der Anwendung steuern. Wenn Sie den **Cloud Scan-Modus** auf **Nur WLAN** einstellen, wird die Cloud-Abfrage nur dann durchgeführt, wenn das Gerät eine WLAN-Verbindung hat. Wenn Sie den **Cloud Scan-Modus** auf **Nicht beim Roaming** einstellen, wird während das Gerät einen Roaming-Vorgang in einem fremden Netzwerk durchführt, niemals eine Cloud-Abfrage durchgeführt.

   b) Legen Sie im **Scan-Intervall** Feld fest, wie oft Scans ausgeführt werden sollen.

   c) Wählen Sie **Benutzer darf Apps vertrauen**, um den Benutzern zu erlauben, Apps zu vertrauen, obwohl diese als Malware erkannt wurden. Der Benutzer kann diese Apps als ignoriert kennzeichnen. In nachfolgenden Scans werden diese Apps nicht als Bedrohungen angezeigt.

4. Unter **Ziele** können Sie folgende Einstellungen festlegen:

   a) Wählen Sie **System Apps scannen**, um System Apps in die Scan-Vorgänge einzubeziehen.

System Apps werden standardmäßig nicht gescannt, da diese durch das Android-Betriebssystem geschützt sind und nicht vom Benutzer entfernt werden können. Sie können jedoch hier das Scannen von System Apps aktivieren.

b) Wenn Sie **Scanne SD-Karte, USB, ...** wählen, werden neben dem standardmäßigen Scan aller auf dem Gerät installierten Anwendungen auch alle Dateien auf SD-Karten (extern und intern) gescannt.

c) Wenn Sie **PUAs erkennen** wählen, wird ein Scan-Vorgang nach PUAs (Potentially Unwanted Applications) durchgeführt.

Potenziell unerwünschte Apps (PUAs) sind Apps, die zwar nicht schädlich sind, jedoch für Unternehmensnetzwerke als ungeeignet angesehen werden. PUAs unterteilen sich in Adware, Dialer, Remote-Administrations-Tools und Hacking Tools. Einige Apps, die unter PUAs fallen, können für manche Benutzer jedoch hilfreich sein.

Wenn Sie diese Option wählen, erkennt Sophos Mobile Security potenziell unerwünschte Apps im Rahmen von Scan-Vorgängen und benachrichtigt den Benutzer entsprechend.

5. Unter **Echtzeitschutz** können Sie folgende Einstellungen festlegen:

a) Standardmäßig scannt Sophos Mobile Security Apps während der Installation auf dem Android-Gerät. Um dieses Verhalten auszuschalten, deaktivieren Sie die Option **Scan bei Installation**.

b) Wählen Sie **Scan-Benachrichtigungen**, um Scan-Benachrichtigungen auf dem Gerät zu erhalten.

c) Wählen Sie **SD-Karte überwachen**, um die SD-Karte auf Änderungen zu überprüfen. Wenn neue Dateien auf der SD-Karte gespeichert werden, werden diese gescannt.

a) Legen Sie im **Webfilter-Modus** Feld die Einstellungen für die Webfilter-Funktion zum Schutz vor unpassendem oder schädlichem Inhalt fest:

- Wenn Sie **Nie** wählen, können Benutzer jede Webseite unabhängig von deren Inhalt auf den Geräten ansehen.
- Wenn Sie **Minimal** wählen, wird eine Warnungsmeldung angezeigt, sobald ein Benutzer eine Webseite mit unpassendem Inhalt öffnet. Der Benutzer kann diese Meldung ignorieren und fortfahren.
- Wenn Sie **Maximal** wählen, werden Webseiten mit unpassendem Inhalt gesperrt.

Die Webseiten werden basierend auf ihrem Inhalt durch SophosLabs kategorisiert. Die Daten werden laufend aktualisiert.

6. Klicken Sie auf die **Speichern** Schaltfläche.

Die Einstellungen gelten für alle Geräte, auf denen die Sophos Mobile Security App installiert ist, in dem Kunden, an dem Sie angemeldet sind. Die in der Sophos Mobile Control Web-Konsole festgelegten Einstellungen können auf dem Endbenutzergerät nicht geändert werden. Sie sind ausgegraut.

26.3 Definieren von Sophos Mobile Security Compliance-Einstellungen

Voraussetzung: Es ist eine Lizenz für die Verwaltung von Sophos Mobile Security über die Sophos Mobile Control Web-Konsole verfügbar.

Sie können Compliance-Einstellungen, die sich auf Sophos Mobile Security beziehen, in der Web-Konsole konfigurieren.

1. Fügen Sie ein neues Set mit Compliance-Einstellungen hinzu oder öffnen Sie ein bereits vorhandenes zum Bearbeiten. Für weitere Informationen siehe *Konfigurieren von Compliance-Einstellungen* (Seite 27).
2. Wechseln Sie in die **Android** Registerkarte.
3. In Feld **Max. SMSec-Scanintervall** können Sie den Höchstabstand zwischen Malware Scans angeben, die von der Sophos Mobile Security App auf dem Gerät durchgeführt werden.
4. Legen Sie im **Malware Apps zugelassen** Feld fest, ob auf Geräten gefundene Malware Apps zulässig sind.
5. Legen Sie im **Verdächtige Apps zugelassen** Feld fest, ob auf Geräten gefundene, verdächtige Apps zulässig sind.
6. Legen Sie im **PUA zugelassen** Feld fest, ob auf Geräten gefundene PUAs (Potentially Unwanted Apps) zulässig sind.
7. Wenn Sie alle erforderlichen Einstellungen konfiguriert haben, klicken Sie auf die **Speichern** Schaltfläche.

26.4 Auslösen eines Scans bei einem bestimmtes Gerät

Voraussetzung: Es ist eine Lizenz für die Verwaltung von Sophos Mobile Security über die Sophos Mobile Control Web-Konsole verfügbar.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Geräte**.

   Die **Geräte** Ansicht mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, wird angezeigt.

2. Klicken Sie auf das **Anzeigen** oder das **Bearbeiten** Symbol neben dem gewünschten Gerät.

   Die **Gerät anzeigen** oder **Gerät bearbeiten** Ansicht wird angezeigt.

3. Klicken Sie auf die **SMSec-Scan starten** Schaltfläche.

Das Gerät wird gemäß den in der Web-Konsole konfigurierten Sophos Mobile Security Einstellungen gescannt.

26.5 Auslösen eines Scans über ein Auftragspaket

Sie können in einem Auftragspaket einen Scan-Auftrag definieren, um zum Beispiel einen Scan auf mehreren Geräten auszulösen und den Scan mit weiteren Aufträgen zu kombinieren.

1. Erstellen Sie ein neues Auftragspaket oder öffnen Sie ein vorhandenes zur Bearbeitung. Für weitere Informationen siehe *Erstellen von Auftragspaketen* (Seite 78).

2. Klicken Sie auf die Schaltfläche **Neuen Auftrag anlegen**.
3. Wählen Sie in der **Typ wählen** Ansicht **SMSec-Scan starten** und klicken Sie auf **Weiter**.

   Die **Auftragseigenschaften bearbeiten** Ansicht wird angezeigt.

4. Geben Sie im **Auftragsname** Feld einen aussagekräftigen Namen für den Auftrag an und klicken Sie auf **Weiter**.

   Der Auftrag wird in der **Auftragspaket bearbeiten** Ansicht unter **Aufträge** angezeigt.

5. Wenn Sie alle erforderlichen Aufträge zum Auftragspaket hinzugefügt haben, klicken Sie auf die **Speichern** Schaltfläche in der **Auftragspaket bearbeiten** Ansicht.

26.6 Einsehen von Sophos Mobile Security Scan-Ergebnissen

Voraussetzung: Es ist eine Lizenz für die Verwaltung von Sophos Mobile Security über die Sophos Mobile Control Web-Konsole verfügbar.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Inventar** auf **Geräte**.

   Die **Geräte** Ansicht mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, wird angezeigt.

2. Klicken Sie auf das **Anzeigen** oder das **Bearbeiten** Symbol neben dem gewünschten Gerät.

   Die **Gerät anzeigen** oder **Gerät bearbeiten** Ansicht wird angezeigt.

3. Wechseln Sie in die **Scan-Ergebnisse** Registerkarte.

   Diese Registerkarte zeigt die Sophos Mobile Security Scan-Ergebnisse. Die unsauberen Pakete, zum Beispiel potenziell unerwünschte Anwendungen, werden in einer Tabelle unterhalb angezeigt. Unter **Threat-Name** können Sie auf die angezeigten Links klicken, um weitere Informationen zur den einzelnen Bedrohungen von SophosLabs abzurufen.

4. Wechseln Sie in die **Richtlinienverletzungen** Registerkarte, um die mit den Scan-Ergebnissen verbundenen Compliance-Verletzungen einzusehen. Die angezeigten Verletzungen richten sich nach den definierten Sophos Mobile Security Compliance-Einstellungen.

27 Anhang: Allgemeine Schaltflächen in der Web-Konsole

Dieser Anhang gibt einen illustrierten Überblick zu allen allgemeinen Schaltflächen der Web-Konsole und deren Funktionen.

Schaltfläche	Name	Beschreibung
	Weiter	Wechselt zur nächsten Ansicht, wenn zum Beispiel ein Vorgangsschritt abgeschlossen ist.
	Zurück	Wechselt zur letzten Ansicht.
	Details	Liefert weitere Informationen zu einem bestimmten Thema.
	Dieses Paket duplizieren	Dupliziert ein Profil/Kommandopaket/Auftragspaket.
	Ja	Bestätigt eine Aktion.
	Nein	Bricht eine Aktion ab.
	Gruppenauswahl	Wechselt zur **Gerätegruppe(n) wählen** Ansicht. In dieser Ansicht können Sie für einen Vorgang eine oder mehrere Gerätegruppen auswählen.
	Gerät(e) wählen	Wechselt zur **Gerät(e) wählen** Ansicht. In dieser Ansicht können Sie für einen Vorgang ein oder mehrere Geräte auswählen.
	Fertigstellen	Wenn Sie die erforderlichen Schritte für einen bestimmten Vorgang abgeschlossen haben, wird über diese Schaltfläche die relevante Aktion ausgeführt.
	Bearbeiten	Öffnet eine Bearbeiten-Ansicht, in der Sie Einstellungen oder Informationen ändern können.
	Speichern	Speichert geänderte Einstellungen.

Schaltfläche	Name	Beschreibung
	Aktualisieren	Aktualisiert den Inhalt einer Tabelle.
	Neuen <Eintrag> erstellen	Fügt einen Eintrag hinzu, zum Beispiel ein Gerät.
	Löschen	Löscht einen ausgewählten Eintrag.
	<Einträge> importieren	Importiert Einträgein Sophos Mobile Control, zum Beispiel Geräte aus einer CSV-Liste.
	Erstellt einen Gerätebericht (CSV-Datei).	Exportiert Geräteinformationen in eine CSV-Datei.

28 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter *http://community.sophos.com/* auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter *http://www.sophos.com/de-de/support.aspx*.
- Laden Sie Dokumentation zu den Produkten unter *http://www.sophos.com/de-de/support/documentation.aspx* herunter.
- Senden Sie eine E-Mail an den technischen Support *support@sophos.de* und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

29 Rechtliche Hinweise

Copyright © 2011 - 2013 Sophos Ltd. Alle Rechte vorbehalten.

Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Sophos ist ein eingetragenes Warenzeichen von Sophos Limited. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.